NATIONS UNIES
BUREAU DE LUTTE CONTRE LE TERRORISME

Protéger les cibles vulnérables contre les attaques terroristes

GUIDE DE BONNES PRATIQUES

Introduction

Programme mondial de lutte contre les menaces terroristes pesant sur des cibles vulnérables

En partenariat avec :
CONSEIL DE SÉCURITÉ DE L'ONU
DIRECTION EXÉCUTIVE DU COMITÉ CONTRE LE TERRORISME (DECT)
UNAOC United Nations Alliance of Civilizations
unicri United Nations Interregional Crime and Justice Research Institute

NATIONS UNIES
BUREAU DE LUTTE CONTRE LE TERRORISME

Protéger les cibles vulnérables contre les attaques terroristes

GUIDE DE BONNES PRATIQUES

Introduction

Programme mondial de lutte contre les menaces terroristes pesant sur des cibles vulnérables

En partenariat avec : CONSEIL DE SÉCURITÉ DE L'ONU
DIRECTION EXÉCUTIVE DU COMITÉ
CONTRE LE TERRORISME (DECT)
UNAOC United Nations Alliance of Civilizations
unicri United Nations Interregional Crime and Justice Research Institute

Table des matières

Préface

Lors du septième examen de la Stratégie antiterroriste mondiale des Nations Unies, l'Assemblée générale des Nations Unies a encouragé le Bureau de lutte contre le terrorisme et les entités signataires du Pacte mondial de coordination contre le terrorisme « à collaborer étroitement avec les États Membres et les organisations internationales, régionales et sous-régionales compétentes pour dégager et mettre en commun les pratiques optimales permettant d'empêcher les attentats terroristes contre des cibles *particulièrement* vulnérables, notamment des infrastructures critiques et des lieux publics (cibles molles) » (paragraphe 74 de la résolution 75/291 de l'Assemblée générale, sans italique dans le texte).

C'est dans ce contexte que le Programme mondial de lutte contre les menaces terroristes pesant sur des cibles vulnérables[1] du Bureau de lutte contre le terrorisme a élaboré le présent document, l'objectif étant d'orienter la protection des sites vulnérables contre les attentats terroristes. Ce document et les quatre modules thématiques spécialisés[2] viennent compléter le *Recueil des bonnes pratiques en matière de protection des infrastructures critiques contre les attaques terroristes*[3]. L'accent est mis sur les « cibles molles » (*soft targets*, soit les lieux publics), des sites qui nécessitent qu'un large éventail d'acteurs adoptent une approche unique en matière de sécurité[4].

Le présent module d'introduction présente des concepts de base, décrit les grands types de menace et donne un aperçu général des rôles et des responsabilités des parties prenantes. Il jette les bases d'un examen plus approfondi de questions particulières, comme la protection des sites religieux, des sites touristiques et des centres urbains, ainsi que la menace que posent les systèmes de drone aérien pour les cibles vulnérables.

---

1 Le Programme est mis en œuvre par le Bureau de lutte contre le terrorisme, en partenariat avec la Direction exécutive du Comité contre le terrorisme, l'Alliance des civilisations de l'Organisation des Nations Unies et l'Institut interrégional de recherche des Nations Unies sur la criminalité et la justice, et en étroite consultation avec d'autres organisations concernées, telles qu'INTERPOL. Voir www.un.org/counterterrorism/fr/vulnerable-targets.

2 Les quatre modules thématiques portent sur la protection des sites religieux, des sites touristiques, des centres urbains et des sites généralement vulnérables aux systèmes de drone aérien.

3 Le Recueil a été élaboré en 2018 par le Groupe de travail sur la protection des infrastructures critiques y compris les cibles vulnérables, Internet et la sécurité du tourisme, sous la supervision de l'Équipe spéciale de lutte contre le terrorisme. En 2019, l'Équipe spéciale a été intégrée au Pacte mondial de coordination contre le terrorisme. Dans le cadre de cette nouvelle structure, ce Groupe de travail et le Groupe de travail sur la prévention des attentats terroristes à l'arme de destruction massive et les interventions en cas d'attentat ont été regroupés afin de créer le Groupe de travail sur les nouvelles menaces et la protection des infrastructures critiques.

4 Le présent document et les quatre modules thématiques respectent la terminologie employée dans la résolution 75/291 de l'Assemblée générale, où les lieux publics sont considérés comme des « cibles molles ».

Le présent module d'introduction et les quatre modules thématiques présentent des études de cas qui illustrent de quelle manière des gouvernements, des entités du secteur privé, des exploitants de sites vulnérables et des organisations de la société civile ont appliqué des principes clés en matière de sécurité, dont des recommandations approuvées par la communauté internationale. Les modules résument également le contenu d'outils (manuels, guides, recueils, etc.) qui éclairent la mise en place de paramètres opérationnels et de politiques propres à rendre les sites moins vulnérables et plus résilients.

Le cadre d'analyse, les études de cas, les outils et les ressources du présent module et des modules thématiques sont le fruit de recherches documentaires approfondies, d'une demande officielle de contributions auprès des 193 États Membres, de discussions avec des experts, des organisations internationales et des partenaires de projet, ainsi que de la participation du Groupe de travail sur les nouvelles menaces et la protection des infrastructures critiques du Pacte mondial de coordination contre le terrorisme[5]. De plus, en 2021, le Bureau de lutte contre le terrorisme a organisé des consultations en ligne auprès de groupes d'experts et de professionnels nationaux et internationaux provenant des États Membres de l'Organisation des Nations Unies, d'organisations internationales et régionales, de groupes de la société civile, du secteur privé et du milieu universitaire. Les contributions du conseiller pour les questions de genre du Bureau de lutte contre le terrorisme et d'un consultant spécialisé dans les droits humains auprès du Service des projets spéciaux et de l'innovation du Bureau[6] se sont également révélées profitables dans le cadre de ce processus.

5 Voir www.un.org/counterterrorism/fr/global-ct-compact.

6 Le présent document et les quatre modules thématiques soulignent la nécessité d'intégrer les questions de genre dans la conception et la mise en œuvre de plans d'action; dans la formation, la mise en pratique et l'exécution d'exercices de sécurité et de plans d'urgence; et dans la planification de la sécurité. Il faut aussi reconnaître et soutenir le rôle des femmes dans la sécurité des cibles vulnérables, combattre les préjugés liés au genre dans l'application de la loi, collaborer pour rendre les milieux urbains plus sûrs pour les femmes, et lutter contre les préjugés sexistes dans les technologies utilisées par les corps policiers et les organes de sécurité. Les considérations adaptées au contexte en ce qui concerne l'égalité des genres doivent être prises en compte au cours du processus de planification, d'exécution et d'évaluation de toutes les mesures décrites dans les modules.

Index des encadrés

Index des études de cas

Index des outils

[1]

Comprendre les concepts de base

1.1 Cibles vulnérables, molles et dures et espaces publics et très fréquentés

Les concepts de cibles vulnérables, molles et dures et d'espaces publics et très fréquentés ne sont que depuis peu utilisés de manière courante dans la lutte antiterroriste[7]. Qui plus est, leur définition ne figure dans aucun cadre juridique international. Dans une certaine mesure, leur signification change selon le contexte et le type de discussion (politique, juridique, opérationnel et technique) dans lequel ils sont employés.

Conformément à la résolution 75/291 de l'Assemblée générale relative au septième examen de la Stratégie antiterroriste mondiale, il

7 L'Assemblée générale a fait mention pour la première fois des « cibles vulnérables » en 2006. Voir résolution 60/288, Annexe, Plan d'action, pilier II (Mesures visant à prévenir et combattre le terrorisme), par. 18, où les États Membres se sont engagés à « [r]enforcer les efforts visant à améliorer la sécurité et la protection des cibles particulièrement vulnérables comme les infrastructures et les lieux publics ».

est tenu pour acquis dans le présent module et les quatre modules thématiques connexes que les cibles vulnérables comprennent les infrastructures critiques et les cibles molles[8] et que la protection de ces cibles doit être assurée en adoptant des approches respectueuses des droits humains et tenant compte des questions de genre[9].

Les cibles molles désignent au sens large les sites vulnérables (stades, centres commerciaux, salles de spectacle, institutions religieuses, zones piétonnes, etc.) qui sont ouverts au public et facilement accessibles et qui, pour ces raisons, ne font délibérément l'objet que de mesures de sécurité limitées, si tant est que de telles mesures existent. Combinée aux foules nombreuses qui se massent souvent sur ces sites, cette particularité en fait des cibles attrayantes pour les acteurs terroristes qui souhaitent maximiser le nombre de victimes, les dégâts et la couverture médiatique sans consacrer trop de ressources à la planification ou la formation[10]. La notion de « cible molle » échappe à toute définition précise, notamment en raison de l'extrême hétérogénéité des lieux qui entrent dans cette catégorie. Les cibles molles peuvent être des installations ou des espaces intérieurs ou extérieurs, permanents ou temporaires. Elles varient par leur taille, leur fonction, leurs caractéristiques physiques, leur emplacement et le profil de leurs utilisateurs.

La « mollesse » de certains lieux contraste avec la « dureté » de certains autres. Dans les discussions sur les politiques, les forces armées et l'application de la loi, les cibles molles sont comparées aux « cibles dures », des sites qui sont généralement occupés ou fréquentés par des agents de l'État et font généralement l'objet d'importantes mesures de sécurité physique (par exemple, les ambassades, les postes militaires, les réunions et sommets internationaux).

Dans une large mesure, la notion de « cibles molles » recoupe celle des « espaces très fréquentés » : la forte densité de personnes à certains endroits ou à proximité de ceux-ci (les visiteurs d'un site touristique, les spectateurs d'un concert, les fidèles d'une cérémonie religieuse, etc.) est un facteur de vulnérabilité potentiellement attrayant pour les acteurs hostiles. La notion de « cible molle » est également fréquemment utilisée comme synonyme d'espaces publics, bien que tous les espaces publics ne soient pas nécessairement (ou invariablement) très fréquentés, et que les espaces très fréquentés ne soient pas forcément non plus des espaces publics ou des sites particulièrement vulnérables (par exemple, plusieurs personnes assistant à un événement dans un bâtiment gouvernemental hautement sécurisé).

8 Ces modules mettent l'accent sur les lieux publics civils ou « cibles molles ». La protection des infrastructures critiques est traitée dans le *Recueil des bonnes pratiques en matière de protection des infrastructures critiques contre les attaques terroristes* (2018), accessible à l'adresse www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_fr.pdf.

9 La section 4.1 donne un aperçu du devoir qu'ont les États Membres de veiller à ce que les mesures antiterroristes soient conformes à l'ensemble des obligations qui leur incombent en vertu du droit international, en particulier des droits humains. Dans le contexte du présent document, les États Membres ont le même devoir pour la conception et la mise en œuvre de mesures de protection des cibles molles.

10 Comme l'a souligné le Comité contre le terrorisme du Conseil de sécurité, les « cibles vulnérables suscitent particulièrement l'intérêt des terroristes car elles sont faciles d'accès et peu sécurisées, mais également du fait du nombre de victimes civiles, du chaos, de la publicité et des répercussions économiques que leur attaque pourrait engendrer » (S/2018/1177, par. 51).

1.2 Cibles molles et infrastructures critiques

Il convient généralement de distinguer la notion de « cible molle » de celle d'« infrastructure critique », bien que ces dernières puissent être « molles » si elles ne sont pas « dures ». Les infrastructures critiques désignent au sens large les biens, les systèmes et les processus qui jouent un rôle capital dans la prestation des services essentiels (santé, eau, télécommunications, transports, énergie, etc.) et dont l'interruption risque de sérieusement compromettre[11] la sécurité et le bien-être social et économique d'une communauté[12].

Les principaux éléments permettant de différencier ces deux notions sont les suivants :

- En général, une cible molle est un emplacement physique; les infrastructures critiques peuvent aussi être des processus, dont les systèmes et réseaux d'information[13];
- Les cibles molles se caractérisent par le fait qu'elles sont ouvertes et accessibles au public. En revanche, les infrastructures critiques sont généralement restreintes d'accès[14];

11 Bien que, techniquement, le secteur du tourisme ne soit généralement pas considéré comme un secteur essentiel, il peut représenter une part très importante du produit intérieur brut national de certains États Membres. Dans ces pays, les répercussions sociales et financières du terrorisme peuvent être tout aussi importantes, voire pires, que celles causées par l'effondrement d'un secteur essentiel.

12 Le *Recueil des bonnes pratiques en matière de protection des infrastructures critiques contre les attaques terroristes* fait mention de plusieurs définitions nationales des « infrastructures critiques » et examine les méthodes utilisées par différents pays pour définir les secteurs et les biens considérés comme essentiels (voir section 2.4.1 – Déterminer le caractère « critique » de certaines infrastructures, p. 36).

13 La notion d'infrastructure d'information critique est essentielle pour comprendre le rôle que jouent les systèmes commandés par ordinateur dans le fonctionnement des centrales énergétiques, des barrages, des ponts, des chaînes d'approvisionnement alimentaire, etc.

14 Le fait que les infrastructures critiques soient fermées au public ne veut pas dire qu'elles sont mieux protégées que les cibles molles. En l'absence de mesures de sécurité adéquates, les infrastructures critiques peuvent être extrêmement vulnérables et donc particulièrement attrayantes pour les acteurs terroristes.

- Des raisons différentes justifient la protection des cibles molles et des infrastructures critiques. Ces dernières sont protégées du fait qu'elles sont essentielles au fonctionnement des pays et que toute perturbation dans un secteur donné peut entraîner d'autres perturbations, culminant potentiellement en une paralysie générale. Cela explique pourquoi la protection des infrastructures critiques – contrairement à la protection des cibles molles – est dirigée non seulement contre le risque d'attaques terroristes, mais également contre les conséquences d'autres comportements humains (intentionnels ou négligents) et, surtout, contre les catastrophes naturelles.

Ces différences conceptuelles donnent à penser que les cadres institutionnels et réglementaires nécessaires à la protection des infrastructures critiques peuvent ne pas s'appliquer automatiquement aux cibles molles. Les critères utilisés par les États Membres pour distinguer les infrastructures critiques de celles qui ne le sont pas en sont la preuve. Ces critères, qui sont souvent fondés sur des modèles de prévision de la gravité, de la durée, de l'étendue géographique et des conséquences économiques des événements perturbateurs, peuvent ne pas être appropriés pour déterminer ce qui constitue une cible molle.

Toutefois, les cibles molles et les infrastructures critiques ont des points communs au chapitre de la protection; l'approche synergique suivante devrait donc s'avérer profitable dans les deux cas :

- Les mesures conçues pour protéger les infrastructures critiques peuvent être une précieuse source d'inspiration pour la protection des cibles molles et vice versa. À la base, bon nombre des outils de sécurité physique utilisés pour contrôler l'accès aux infrastructures critiques (postes de garde, clôtures, détecteurs de métaux, etc.) servent généralement à régir également l'accès du public aux cibles molles[15];
- La gestion d'une attaque contre une infrastructure critique peut fournir d'importants enseignements en vue d'atténuer les risques auxquels sont exposés les cibles molles et de gérer les crises les concernant;
- La protection des infrastructures critiques et celle des cibles molles reposent sur la nécessité pour les exploitants des sites et les autorités publiques d'adopter des approches de gestion des risques et des crises. Qu'il s'agisse d'infrastructures critiques ou de cibles molles, l'évaluation des menaces au plan national et les mesures d'intervention après attaque se recoupent beaucoup, quand elles ne sont pas les mêmes; il en va de même pour les acteurs chargés d'évaluer ou d'intervenir. En outre, comme les infrastructures critiques et les cibles molles sont la plupart du temps détenues et exploitées par des intérêts privés, l'établissement de partenariats public-privé est, dans les deux cas, un élément central des efforts de préparation et de protection;
- La proximité entre la protection des infrastructures critiques et celle des cibles molles nécessite une étroite coordination sur les plans politique, institutionnel et opérationnel. Les infrastructures critiques sont ce qui permet le plus souvent aux cibles molles de fonctionner. Par exemple, les événements sportifs ne peuvent pas se dérouler si l'électricité est coupée. Toute interruption des services de base, comme l'électricité, peut laisser le public d'une salle de concert dans le noir et interrompre la représentation, bien sûr, mais elle peut aussi faire partie d'une stratégie visant à compliquer l'évacuation lors d'une attaque terroriste. Par ailleurs, une attaque terroriste réussie contre un site touristique ou

15 Le concept de « ville intelligente » et les solutions technologiques connexes visant à rendre les villes modernes plus sûres sont d'autres exemples de mesures de sécurité qui peuvent être employées pour protéger aussi bien les infrastructures critiques que les cibles molles. Par exemple, les capteurs numériques de détection d'armes à feu peuvent être utiles pour protéger des éléments aussi divers qu'un marché en plein air, un bâtiment gouvernemental ou un réseau de transport.

religieux bondé peut provoquer l'effondrement d'infrastructures critiques, voire de tout un secteur essentiel. Par exemple, les hôpitaux peuvent rapidement se remplir au-delà de leur capacité et les réseaux de communication peuvent se retrouver submergés sous les demandes des utilisateurs. Les attaques contre des cibles molles peuvent avoir des répercussions particulièrement graves sur les infrastructures critiques en milieu urbain, où les deux coexistent et interagissent dans des espaces complexes et densément peuplés, soulignant ainsi la nécessité d'une approche qui considère les deux comme faisant partie d'un seul système à multiples facettes.

Encadré 1.
Aligner les mesures de protection des cibles civiles et des infrastructures critiques

« Les infrastructures critiques, telles que le réseau de distribution électrique, les barrages et les installations gouvernementales, resteront haut placées sur la liste des cibles des terroristes. Dans bon nombre de pays, les cibles civiles font partie du cadre des infrastructures critiques. Ainsi, le système de gestion des risques posés aux infrastructures englobe également la menace contre les cibles civiles. Par exemple, les attentats contre les personnes se trouvant dans une gare ferroviaire s'inscrivent dans un ensemble de scénarios possibles visant les systèmes de transport (aérien, ferroviaire, maritime). La plupart des principes clés sur lesquels s'appuient les gouvernements pour la protection de leurs infrastructures critiques peuvent également être efficaces pour la protection des cibles civiles [...] La protection des cibles privées, la sécurité des infrastructures critiques et la résilience exigent toutes un même cadre politique et pratique contribuant au niveau de préparation, fondé sur : la prévention, la protection, l'atténuation des effets, l'intervention et le relèvement. Ces mesures doivent se renforcer mutuellement [...] En tout état de cause, les évaluations des cibles civiles devraient être effectuées conjointement à celle de la capacité d'un gouvernement à mettre au point des plans d'intervention et des partenariats en vue de protéger les infrastructures critiques. Dans certains cas, les cibles civiles peuvent coïncider avec les infrastructures critiques (installations commerciales) mais dans d'autres, elles sont tout à fait distinctes (secteur énergétique). »

Source : Mémorandum d'Antalya (2017), Bonne pratique n° 5.

[2]

La menace terroriste qui pèse sur les cibles vulnérables

Au cours des dernières années, la présence d'une menace terroriste persistante pesant sur les sites où de grandes foules se massent a été régulièrement mise en évidence par les services de renseignement et de maintien de l'ordre partout dans le monde. Dans bien des cas, le public est généralement conscient de cette menace puisque les organisations terroristes ont publiquement encouragé les attaques contre ces lieux ou menacé de les attaquer[16].

Les terroristes risquent de se tourner vers des cibles molles en réaction aux mesures de sécurité renforcées qui rendent plus difficiles à attaquer les cibles dures, comme les bâtiments gouvernementaux et les installations militaires, par exemple. La situation peut être assimilée à un « effet de déplacement » : l'amélioration de la sécurité et du maintien de l'ordre dans une région donnée peut faire en sorte que l'activité criminelle se déplace vers un territoire moins contrôlé. De même, après l'adoption des mesures de sécurité de plus en plus strictes avant l'embarquement en réponse à la menace terroriste sur l'aviation civile, les groupes terroristes ont détourné leur attention vers les zones environnantes, moins protégées[17].

Parallèlement, comme le souligne le Mémorandum d'Antalya du Forum mondial de lutte contre le terrorisme, l'« accroissement récent du nombre d'attentats commis à l'aide de couteaux ou de poids lourds montre que l'on s'écarte de la traditionnelle implication d'un individu armé ou d'un groupe de personnes armées, avec parfois des attentats-suicides; cela démontre une certaine souplesse et une disposition à accepter d'avoir un nombre restreint de victimes[18] ».

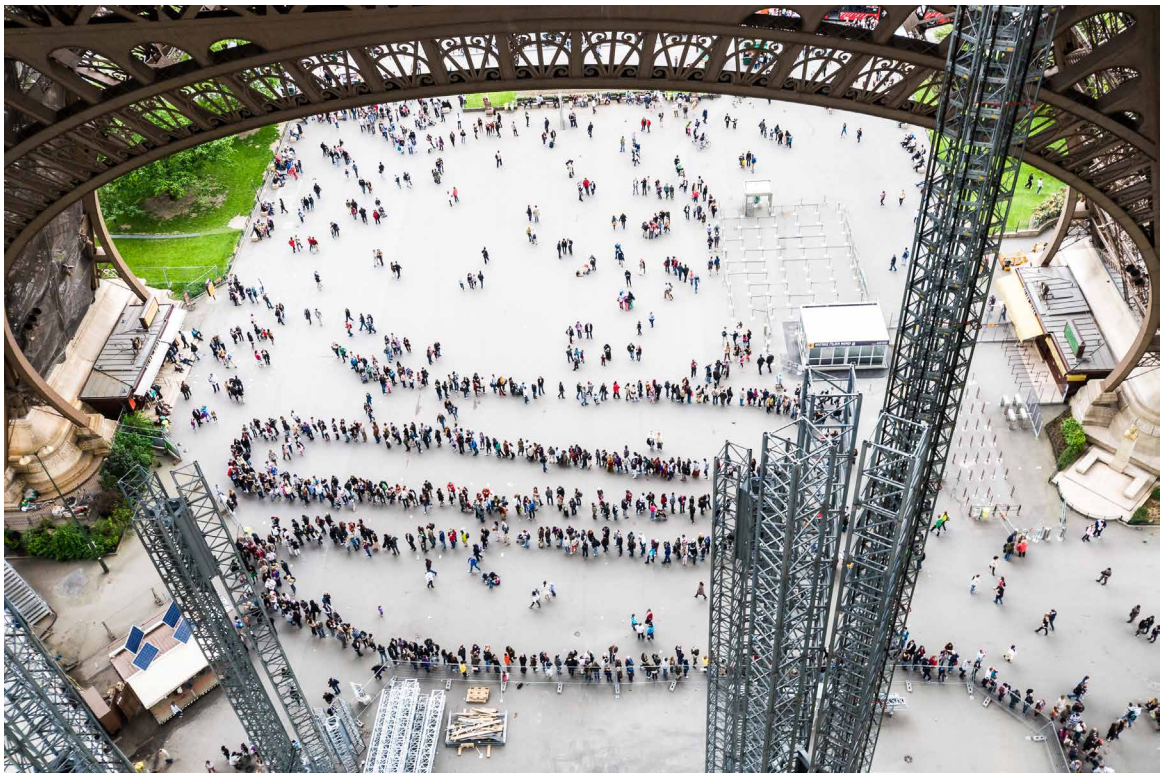
Bien que l'utilisation d'armes rudimentaires ait caractérisé plusieurs attaques récentes, on ne peut exclure la possibilité que des acteurs terroristes cherchent à employer des armes de destruction massive pour s'attaquer à des cibles molles. La tentative la plus connue à cet égard est l'attaque au gaz sarin perpétrée en 1995 par le groupe terroriste Aum Shinrikyo dans le métro de Tokyo[19].

16 Par exemple, en novembre 2016, dans son magazine en ligne, l'État islamique (EIIL) a invité ses sympathisants à cibler les grandes assemblées et célébrations en plein air, les rues bondées de piétons, les marchés extérieurs, les festivals, les défilés et les manifestations politiques.

17 L'attentat à la bombe survenu à Bruxelles en 2016 illustre bien ces propos. En frappant un endroit bondé de passagers et de valises (la zone d'enregistrement de l'aéroport, avant les contrôles de sécurité), les terroristes ont réduit au minimum le risque de voir leur plan déjoué, tout en maximisant leurs chances de causer des dégâts importants.

18 Les véhicules piégés que les terroristes stationnent à proximité de cibles molles en vue de les faire exploser représentent une menace particulière. Par le passé, de nombreux groupes terroristes ont utilisé des ambulances à cette fin en exploitant leur caractère apparemment inoffensif.

19 Un incident moins célèbre s'est produit en 1984, alors que des buffets à salades ont été intentionnellement contaminés à la salmonelle dans 10 restaurants de l'Oregon, aux États-Unis, par un groupe cherchant à influencer une élection locale. Cet incident illustre la relative facilité avec laquelle des acteurs hostiles peuvent potentiellement perpétrer une attaque bioterroriste contre des cibles molles.



Les cibles molles continuent également d'être le théâtre de prise d'otages[20] et pourraient être utilisées par les terroristes pour acquérir des matières dangereuses qui serviront dans des attentats perpétrés ailleurs[21].

La nature et la gravité de la menace qui pèse sur les cibles molles dépendent de divers facteurs locaux, de même que du profil des acteurs violents qui cherchent à y causer des dommages et à blesser ou tuer les personnes présentes. Diverses considérations peuvent influencer le choix des terroristes d'attaquer un site plutôt qu'un autre, telles que leurs griefs personnels contre des groupes particuliers (comme certaines communautés religieuses, les touristes de certains pays, la perception d'activités amorales) et le degré de vulnérabilité réel ou perçu du site. D'un point de vue général, les acteurs terroristes peuvent décider d'attaquer des cibles molles pour diverses raisons[22]. Outre celles qui sous-tendent généralement la décision de s'en prendre à des sites vulnérables (par exemple, la présence de grandes foules, la faiblesse des mesures de sécurité – voire leur inexistence –, la proximité de la zone d'opération ou du point d'accès du groupe, la possibilité d'obtenir rapidement une couverture médiatique), les motifs suivants peuvent également expliquer cette décision :

- Pour compenser une faiblesse : si un groupe terroriste ou un acteur isolé ne dispose pas des ressources ou des capacités de planification nécessaires pour mener à bien une attaque contre une cible dure, il peut se rabattre sur une cible molle;

20 Par exemple, les terroristes qui ont pris 850 personnes en otage au théâtre Doubrovka de Moscou ont fait des revendications politiques au Gouvernement russe comme condition à la libération des otages. Dans le nord-ouest du Nigéria, les fréquents enlèvements de masse de filles et de garçons dans les internats sont généralement commis dans le but de demander une rançon.

21 Après avoir observé la faiblesse de la sécurité dans des installations médicales où étaient stockées des substances radioactives, le Gouvernement des États-Unis a publié en 2012 un rapport exposant le risque que des acteurs hostiles exploitent les failles de sécurité pour voler ces substances et fabriquer une arme radiologique [voir États-Unis d'Amérique, Government Accountability Office (2012)].

22 Voir Hesterman (2019), p. 23-26.

- Comme solution de dernier recours : un groupe terroriste qui voit son pouvoir d'attraction ou ses capacités opérationnelles affaiblis peut se tourner vers des cibles molles faciles à attaquer pour regagner en crédibilité et attirer de nouvelles recrues;
- Pour mettre à l'essai une nouvelle stratégie, arme ou tactique : les cibles molles peuvent servir de terrains d'essai pour préparer des opérations plus importantes;
- Pour bénéficier d'une plus grande marge de manœuvre : les cibles molles peuvent laisser plus de place à l'improvisation au cas où il faudrait modifier le plan initial pour quelque raison que ce soit.

[3]

La vulnérabilité des cibles molles face aux attaques terroristes

Chaque type de site présente un ensemble unique de vulnérabilités qui découlent, dans une large mesure, des particularités des personnes qui gèrent, exploitent, visitent ou fréquentent le site et des ressources à leur disposition. En effet, la plupart des religions et des communautés religieuses ont pour politique d'accueillir « à bras ouverts » les visiteurs inconnus et de ne pas s'enquérir de leur identité, de leur religion ou de leur origine. En outre, pour mener à bien leurs attaques sur un site religieux, les auteurs peuvent tirer parti de l'effet de surprise, particulièrement lorsque les fidèles sont plongés dans leur propre pratique spirituelle et ne prêtent pas attention aux autres. Heureusement, les habitués d'un site religieux pourront généralement accéder plus facilement aux issues et aux portes de secours que les touristes qui visitent un point d'attraction.

Les vulnérabilités varient également fortement en fonction du contexte socioéconomique, de l'emplacement, de l'environnement et des caractéristiques physiques des sites. Par exemple, il peut être plus difficile de réussir une attaque en libérant des agents toxiques dans un marché en plein air que dans une installation intérieure, comme une salle de spectacle. En revanche, le public dans une salle de spectacle sera nettement moins exposé à une attaque par drones que la foule d'un marché extérieur.

Malgré ces différences, on peut définir des vulnérabilités qui recoupent la plupart des secteurs et qui dépendent de divers facteurs culturels, institutionnels, juridiques et financiers.

- *Facteurs culturels :* les vulnérabilités peuvent résulter d'une réticence à renforcer la sécurité, du fait que la probabilité ou l'impact d'une attaque terroriste est sous-estimé. Certains propriétaires et exploitants d'établissements peuvent être réticents face au changement et portés à ne pas mettre en place de solides mesures de sécurité qui nuirait à l'expérience des fidèles, des touristes, des visiteurs des centres commerciaux, des participants à des événements culturels, etc.

  Un autre facteur potentiellement pertinent est le relâchement : les exploitants, le public et les autres acteurs concernés peuvent avoir du mal à accepter de maintenir les mesures de sécurité à long terme, au-delà de la période de vigilance accrue qui suit généralement un attentat. Les acteurs de la sécurité eux-mêmes peuvent éveiller les soupçons ou ne pas être bien accueillis dans certains milieux (par exemple, certaines congrégations religieuses).

  Il peut aussi y avoir des vulnérabilités particulières qui résultent des barrières culturelles (origines, attentes et mentalités différentes) et des réticences que suscitent ces barrières quant à l'adoption de mesures de sécurité plus strictes. Il est

donc essentiel d'établir des partenariats public-privé efficaces parmi les parties prenantes appelées à collaborer à la protection des sites vulnérables, ce qui n'est pas donné d'emblée[23].

- *Facteurs institutionnels et juridiques :* l'échange d'informations est un élément essentiel de tout système de gestion des risques et des crises qui réussit à protéger les cibles vulnérables efficacement; toutefois, cet échange risque d'être compromis par le manque de coordination interinstitutions attribuable aux lacunes réglementaires, à une répartition des tâches imprécise, etc. En outre, les services de renseignement peuvent se heurter à des obstacles juridiques lorsqu'ils veulent divulguer des informations classifiées aux exploitants de sites vulnérables.

  Sur le terrain, des malentendus peuvent survenir entre les propriétaires et les locataires de sites vulnérables ou entre les exploitants et les entreprises voisines quant à savoir à qui revient la responsabilité d'améliorer la sécurité ou de gérer le personnel de sécurité dans ce qu'on appelle les « zones grises », c'est-à-dire les espaces dont la propriété est contestée ou qui n'ont pas de propriétaire clairement désigné. De telles situations peuvent entraîner une incapacité à mettre en œuvre les mesures de sécurité préventives et potentiellement nuire aux mesures d'intervention à la suite d'un incident.

- *Facteurs financiers :* de nombreux sites vulnérables disposent de budgets de sécurité limités. Il peut se révéler coûteux de déployer des mesures de sécurité lorsqu'il faut, pour ce faire, apporter des ajouts ou des modifications physiques à l'infrastructure, retenir les services de nouvelles entreprises de sécurité ou embaucher des employés qui doivent être formés. Il est possible, en outre, que ces sites ne puissent bénéficier d'aide (financement, subventions, allégements fiscaux, etc.) pour financer l'amélioration de la sécurité. Les exploitants de sites vulnérables qui font face à d'importantes contraintes budgétaires peuvent choisir, par exemple, d'investir leurs maigres ressources dans des activités de marketing qui leur seront rapidement profitables plutôt que dans la restructuration de la sécurité à long terme, omettant ainsi de corriger des vulnérabilités facilement exploitables.

23 Les autorités publiques peuvent parfois se montrer intransigeantes et demander aux exploitants de sites d'apporter des améliorations à la sécurité qui s'avèrent financièrement contraignantes. De leur côté, les exploitants peuvent hésiter à s'engager dans des partenariats public-privé solides et durables en raison de divers facteurs : incapacité à voir la valeur commerciale d'un tel partenariat, doutes quant aux motifs de l'État, manque d'intérêt vu l'absence de réglementation engageant le secteur privé, etc.

[4]

Atténuation des risques et intervention : rôles des parties prenantes

Le paradigme fondamental de la protection des cibles vulnérables – quels qu'en soient le type, la taille et la fonction – contre les actes terroristes réside dans la planification coordonnée des mesures de sécurité, ce qui implique que les risques et les crises sont gérés par les exploitants et les autorités gouvernementales, tant au niveau national que local.

Le Bureau des Nations Unies pour la prévention des catastrophes définit la gestion des risques comme l'« approche systémique et pratique managériale pour limiter les dommages et les pertes potentiels [...] La gestion des risques comprend l'évaluation des risques et leur analyse, ainsi que la mise en œuvre de stratégies et d'actions spécifiques pour les contrôler, les réduire et les transférer. »[24]

Il ne faut pas sous-estimer l'importance d'adopter des approches de gestion des risques étroitement coordonnées faisant appel à tous les ordres de gouvernement et aux autres acteurs concernés. Dans sa résolution 75/291, l'Assemblée générale « engage [les États Membres] à envisager d'élaborer des stratégies de réduction des risques posés par les attaques terroristes au regard des infrastructures critiques, ou à améliorer celles qu'ils ont déjà adoptées, en prévoyant notamment d'évaluer et de faire

24 Voir Stratégie internationale de prévention des catastrophes, Terminologie pour la réduction des risques de catastrophe (2009).

mieux connaître ces risques, de prendre des mesures de préparation, y compris pour intervenir de manière efficace en cas d'attaque, de favoriser une meilleure interopérabilité dans la gestion de la sécurité et des conséquences, et de faciliter des échanges fructueux entre toutes les parties prenantes » (par. 71). De plus, comme souligné dans le Mémorandum d'Antalya du Forum mondial de lutte contre le terrorisme, les « données à partir desquelles réaliser l'évaluation proviennent de sources nombreuses et variées. Les évaluations nationales effectuées par des experts gouvernementaux en matière de sécurité incluront des informations sensibles et classifiées qui ne sont accessibles qu'à des représentants nationaux officiels. Il convient d'intégrer ces informations aux données ouvertement accessibles et aux renseignements fournis par les entreprises de sécurité ou le secteur privé, de sorte qu'ils soient à la disposition des forces de sécurité locales qui en ont besoin. L'analyse du risque est utilisée tant dans le secteur public que dans le privé en vue d'identifier les vulnérabilités des infrastructures et de les atténuer, tout en les intégrant dans leurs procédures opérationnelles normalisées et leurs plans d'intervention. » (p. 6, Bonne pratique n° 3)

La gestion des crises, quant à elle, fait largement référence aux processus qui doivent être enclenchés lorsqu'un incident se produit. Les trois principales étapes de la gestion des crises sont les suivantes : élaborer des plans d'intervention ou d'intervention d'urgence; identifier une crise; faire face à la crise et la régler[25].

Les sections qui suivent décrivent brièvement les rôles des différentes parties prenantes dans la protection des cibles vulnérables dans le cadre d'un modèle de gestion des risques et des crises. La même approche basée sur les parties prenantes est adoptée dans les modules spécialisés, qui examinent comment les acteurs gouvernementaux et non gouvernementaux peuvent contribuer à la protection des sites religieux et touristiques, des centres urbains, ainsi que des sites vulnérables à l'utilisation de systèmes de drone aérien à des fins terroristes.

4.1 États Membres

Tous les services de l'État doivent participer à la protection des cibles vulnérables en fonction des prérogatives qui leur sont dévolues dans le droit national.

Les mesures générales de lutte contre le terrorisme sont les outils de base qu'il convient d'utiliser. Tous les outils et les politiques antiterroristes doivent être exploités dans le plein respect des droits humains, des normes d'égalité des genres et du droit international. Ces outils et politiques comprennent notamment : des mesures visant à lutter contre l'extrémisme violent; des stratégies complètes et adaptées en matière de poursuites, de réadaptation et de réintégration; des mesures visant à empêcher l'accès des terroristes aux armes; des mécanismes de coopération internationale et d'échange d'informations découlant des traités internationaux; des programmes de sécurité et de gestion des frontières visant à empêcher les mouvements transfrontaliers de terroristes et à endiguer le flux de combattants terroristes étrangers; des mesures liées aux expéditions de biens à double usage (pour la fabrication d'engins explosifs improvisés, entre autres).

25 Le *Recueil des bonnes pratiques en matière de protection des infrastructures critiques contre les attaques terroristes* donne des renseignements et orientations supplémentaires sur la gestion des risques et des crises qui s'appliquent tant aux mesures de protection des infrastructures critiques qu'à celles visant les cibles molles (voir section 2.6).

Les principaux rôles et responsabilités qui sont liés, d'une part, à la protection des cibles vulnérables qui relèvent des pouvoirs d'élaboration des politiques et d'application des lois des pays, et d'autre part, à la collecte et l'analyse d'informations et de renseignement en soutien à la lutte contre le terrorisme sont décrits ci-après.

Encadré 2.
La protection des espaces publics : conclusions du Conseil de l'UE

En juin 2021, le Conseil de l'Union européenne (Justice et affaires intérieures) a adopté un certain nombre de recommandations à l'intention des États membres de l'Union européenne concernant la protection des espaces publics contre les actes terroristes. La liste suivante résume les principales recommandations formulées :

- Œuvrer en faveur de la mise en œuvre et/ou du renforcement de stratégies nationales, régionales et locales visant à accroître la résilience des communautés locales et des espaces publics;
- Soutenir des initiatives visant à établir une communication opérationnelle et interopérable à l'échelle de l'Union européenne qui soit sûre pour permettre aux services répressifs et autres praticiens de la sécurité d'assurer une protection adéquate et de réagir de manière appropriée en cas de coopération transfrontière en matière d'espaces publics et d'événements majeurs;
- Examiner les cadres juridiques nationaux en vue de restreindre le port non légitime d'armes blanches dans les espaces publics et lors de grands événements;
- Étudier et analyser les orientations et outils en matière de sécurité destinés aux opérateurs de location de véhicules afin de prévenir et d'atténuer le risque d'attaques menées à l'aide de véhicules dans des espaces publics;
- Examiner la législation nationale et la réglementation locale afin de s'assurer qu'elles contiennent des dispositions claires en ce qui concerne les exigences administratives et les responsabilités des personnes qui planifient et gèrent la sécurité des espaces publics;
- Continuer à planifier et à organiser des exercices pratiques et des formations communes entre les autorités locales, les services répressifs, la protection civile, les urgences médicales, les entreprises privées, les sociétés de sécurité privées et d'autres parties prenantes afin d'améliorer la préparation et la réaction des services répressifs et des services de première intervention;
- Intégrer la prévention de la criminalité par les techniques de conception environnementale au niveau local et au moyen de partenariats et de projets public-privé, en tant que mécanisme de protection des espaces publics, à savoir la prévention des attaques au véhicule-bélier, des explosions, des matériaux chimiques, biologiques, radiologiques et nucléaires, des engins incendiaires improvisés, des tireurs actifs et d'autres modes opératoires dans des lieux tels que les gares ferroviaires et souterraines, les zones publiques des aéroports internationaux, les lieux de culte, les zones commerciales, les attractions touristiques (par exemple, les monuments et les musées), les universités et les écoles, ainsi que d'autres lieux que l'évaluation des risques pourrait suggérer.

Source : https://data.consilium.europa.eu/doc/document/ST-9545-2021-INIT/fr/pdf.

4.1.1 Obligation pour les États Membres d'adopter une approche respectueuse des droits humains et tenant compte des questions de genre pour lutter contre les menaces terroristes pesant sur les cibles molles

Le terrorisme représente une menace importante pour la paix et la sécurité internationales, de même que pour les droits humains et le développement social et économique. En vertu du droit international des droits humains et de l'obligation qui en découle de protéger les droits à la vie et à la sécurité des personnes, les États Membres sont tenus de prendre des mesures efficaces pour prévenir et contrer le terrorisme. Cette obligation est particulièrement importante compte tenu des répercussions potentielles que les attaques contre des cibles molles peuvent avoir sur la population, notamment du fait que ces cibles sont des lieux ouverts et accessibles au public, où de grandes foules se rassemblent.

Pour s'acquitter de leur devoir de protéger les droits humains, les États ont l'obligation de prendre les mesures nécessaires et adéquates pour prévenir, réprimer et sanctionner les activités qui compromettent ces droits, comme les menaces à la sécurité nationale et les crimes violents, y compris le terrorisme. À cet égard, les États devraient s'appuyer entre autres sur la Stratégie antiterroriste mondiale des Nations Unies, qui souligne que lutter efficacement contre le terrorisme et garantir le respect des droits humains ne sont pas des objectifs contradictoires mais complémentaires, qui se renforcent mutuellement. En effet, la promotion et la protection des droits humains sont en elles-mêmes un pilier et une nécessité transversale essentielle à la réussite des quatre composantes de la Stratégie. Le Conseil de sécurité a également affirmé à maintes reprises que les États doivent veiller à ce que toutes les mesures prises pour lutter contre le terrorisme soient conformes aux obligations découlant du droit international, en particulier du droit international des droits de l'homme, du droit international des réfugiés et du droit international humanitaire. De plus, dans sa résolution 2178 (2014), le Conseil de sécurité a noté que « le fait de se soustraire à ces obligations internationales particulières comme à d'autres, dont celles résultant de la Charte des Nations Unies, est un des facteurs contribuant à une radicalisation accrue et favorise le sentiment d'impunité ».

En outre, selon les dispositions pertinentes des résolutions du Conseil de sécurité, toutes les mesures prises pour prévenir et combattre le terrorisme doivent être conformes aux obligations qui incombent aux États en vertu du droit international, en particulier du droit international des droits humains, du droit international des réfugiés et du droit international humanitaire. Les stratégies de lutte contre le terrorisme doivent également tenir compte des sensibilités liées au sexe et à l'âge, de l'intérêt supérieur de l'enfant et du fait que le terrorisme et l'extrémisme violent pouvant conduire au terrorisme portent particulièrement atteinte aux droits fondamentaux des femmes et des filles (voir S/2018/1177, annexe, par. 8.)

Pour endiguer les menaces terroristes contre les cibles molles, les autorités publiques peuvent prendre des mesures temporaires susceptibles de limiter certains droits, pourvu que les restrictions imposées respectent les conditions prescrites par le droit international des droits humains. Les mesures prises à cet égard doivent véritablement répondre à la menace en question, être indispensables compte tenu de la situation, avoir un fondement juridique clair et être proportionnelles aux objectifs légitimes poursuivis. Dans ce contexte, les États doivent veiller à mettre en place des mesures de protection satisfaisantes contre toute ingérence arbitraire ou disproportionnée. Afin de réellement respecter ces obligations, les États sont vivement encouragés à évaluer régulièrement, du point de vue des droits humains, les mesures prises pour faire face à la menace terroriste

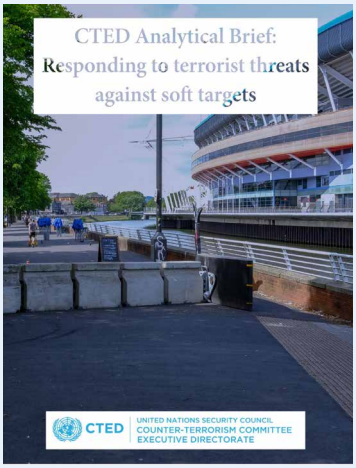
pesant sur les cibles molles et à veiller à ce qu'elles soient fondées sur des données probantes et donc efficaces et à ce qu'elles ne renforcent pas l'exclusion, les préjugés ou les partis pris ni n'empêchent certains groupes ou populations d'utiliser l'espace ou d'y accéder. De même, l'intégration des questions de genre dans la protection des cibles vulnérables est essentielle pour des stratégies d'atténuation des risques efficaces et efficientes, puisqu'elle permet de tenir compte non seulement des besoins en matière de sécurité propres aux femmes, aux hommes, aux garçons et aux filles, mais aussi de la manière dont les relations, la dynamique et les stéréotypes sexospécifiques sous-jacents influencent les modèles de sécurité et d'insécurité et les vulnérabilités.

4.1.2 Décideurs

Dans le respect des paramètres établis par une stratégie gouvernementale globale, les différents ministères et départements doivent concevoir leur engagement en fonction des caractéristiques des sites dont ils sont responsables (sur le plan des politiques, de la réglementation, des inspections, etc.). En outre, des partenariats devront être établis avec différentes catégories de parties prenantes. Par exemple, la protection des sites religieux nécessitera un dialogue soutenu avec les chefs religieux, alors qu'il faudra faire appel au secteur du tourisme pour prévenir les attaques terroristes contre les points d'attraction. Pour assurer la sécurité des centres urbains vulnérables, il faudra donner les moyens adéquats aux autorités municipales; et pour endiguer la menace que les terroristes utilisant des systèmes de drone aérien font peser sur les cibles molles, il faudra que les organismes gouvernementaux et les fournisseurs de technologies de lutte contre ces systèmes se concertent.

S'il est vrai que les différents types de sites vulnérables nécessitent des interventions politiques et réglementaires adaptées, les gouvernements se doivent néanmoins de concevoir une approche globale en vue d'en assurer la protection. Une telle approche devrait permettre de faire le point sur les priorités et les difficultés conjointes, de cerner les besoins opérationnels communs et d'optimiser l'utilisation des ressources et des outils disponibles aux fins de prévention, d'intervention et de relèvement.

Outil 1.
Responding to Terrorist Threats against Soft Targets – CTED Analytical Brief (Notes analytiques de la DECT sur la lutte contre les menaces terroristes pesant sur des cibles vulnérables)
(www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted-analytical-brief-soft-targets.pdf)



La Direction exécutive du Comité contre le terrorisme (DECT) a préparé ces notes analytiques conformément à la résolution 2395 (2017) du Conseil de sécurité, qui l'a chargée d'effectuer des travaux d'analyse sur les questions et tendances

(suite)

émergentes et de mettre ces analyses à la disposition de l'ensemble du système des Nations Unies. Le document souligne également l'importance de faire participer la société civile aux initiatives de protection des cibles molles, ainsi que la nécessité d'améliorer l'échange d'informations et de renforcer la confiance afin d'accroître la résilience sans divulguer de renseignements confidentiels ni perturber le mode de vie de la population.

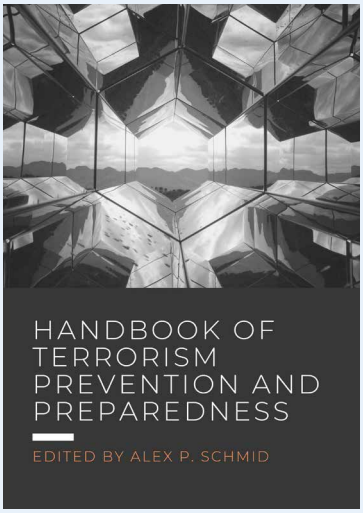
Outil 2.
Mémorandum d'Antalya sur les bonnes pratiques relatives à la protection des cibles civiles dans le contexte de la lutte antiterrorisme – Forum mondial de lutte contre le terrorisme (2017)
(www.thegctf.org/About-us/GCTF-framework-documents)

Les bonnes pratiques reprises dans le Mémorandum s'inscrivent dans le cadre de l'initiative relative à la protection des cibles vulnérables du Forum mondial de lutte contre le terrorisme, qui a pour but d'informer et d'orienter les gouvernements et les intervenants du secteur privé œuvrant de concert à l'élaboration de politiques, pratiques, lignes directrices, programmes et approches concernant la protection des populations face aux attaques terroristes contre des cibles civiles (*soft targets*). Reconnaissant qu'il n'existe pas de plan ou de stratégie en mesure de protéger toutes les cibles potentielles, le Mémorandum cherche à dresser une synthèse du savoir-faire et de l'expérience recueillis dans ce domaine lors de divers ateliers régionaux tenus en 2016 et 2017.

Les 13 bonnes pratiques qui en sont issues ont été regroupées en 3 principaux thèmes :

1. Comprendre la menace afin d'identifier et de hiérarchiser les cibles civiles à partir d'évaluations continues du risque et d'un partage d'information avéré et effectif qui promeuvent la coopération et la collaboration pratiques entre pouvoirs publics à tous les échelons (international, national, régional et local);
2. Édifier des partenariats public-privé afin d'habiliter et améliorer la coopération dans le domaine de la sécurité, et susciter la participation du public et des entreprises au moyen de messages clairs et cohérents sur la nature de la menace et le niveau adéquat de préparation;
3. Préparer, planifier et protéger en priorisant les ressources, l'engagement, les exercices et la formation afin de rehausser le niveau de sensibilisation et de préparation des pouvoirs publics, du secteur privé et du public à la prévention, à la réponse à apporter et au retour à la normale.

Outil 3.
Handbook of Terrorism Prevention and Preparedness (Manuel de prévention et de préparation au terrorisme) – Centre international pour la lutte contre le terrorisme
(https://icct.nl/handbook-of-terrorism-prevention-and-preparedness)



Préparé par le Centre international pour la lutte contre le terrorisme, ce manuel est un important outil de référence qui aborde divers aspects de la lutte préventive contre le terrorisme, allant de la prévention de la radicalisation et des actes préparatoires à la préparation nécessaire en vue d'atténuer les conséquences d'un attentat.

Le chapitre 27, plus particulièrement, porte sur les niveaux de mesures préventives requis pour protéger les cibles molles contre les attaques terroristes, en partant du principe que bien que les niveaux individuels puissent s'avérer insuffisants pour contrer de telles attaques, combinés, ils peuvent devenir un puissant outil de prévention. Le manuel définit 13 niveaux de mesures préventives pour assurer la protection en temps utile et en aval des cibles molles[26] :

Niveau 1 : Entreprendre la collecte permanente de renseignements tirés de sources publiques traditionnelles (presse écrite, radio, télévision, études universitaires, rapports d'organisations non gouvernementales, etc.) par l'entremise d'organismes de surveillance professionnels;

Niveau 2 : Surveiller les activités menées en ligne par des extrémistes, notamment dans les médias sociaux et sur le *dark* et le *deep* Web, qui peuvent avoir des conséquences potentiellement importantes (par exemple, les discours haineux qui peuvent être un facteur prédictif de crimes haineux et de terrorisme);

Niveau 3 : Effectuer la collecte de renseignements en procédant à la surveillance et à l'interception des communications d'individus et de groupes extrémistes connus et présumés et de leurs parrains (en mettant notamment sur écoute leurs téléphones, leurs ordinateurs, leurs voitures et leurs domiciles);

Niveau 4 : Faire appel à des agents spécialisés pour des groupes violents ou y recruter des informateurs (par exemple, des terroristes ayant réintégré leur groupe après avoir été libérés de prison), et organiser des opérations d'infiltration, là où celles-ci sont légales;

Niveau 5 : Assurer l'échange de renseignements finis, c'est-à-dire non bruts (veille automatique et humaine), au sein des organismes gouvernementaux et entre eux, de même qu'avec des services de renseignement et de sécurité de confiance à l'étranger;

26 La prévention en temps utile cible les campagnes terroristes, tandis que la prévention en aval cible les attentats pris individuellement.

(suite)

Niveau 6 : Analyser la propagande terroriste et préparer des contre-discours et une contre-propagande étayés par des actions crédibles afin de prévenir et de contrer la radicalisation;

Niveau 7 : Encourager les membres de la famille et les amis des jeunes hommes et femmes radicalisés à faire part de leurs inquiétudes, en toute confidentialité, à un organisme de confiance (et non aux services de police ou de renseignement), tout en leur assurant que leurs proches ne seront pas arrêtés, mais bien mis en contact avec des conseillers travaillant dans des programmes d'encadrement ou de déradicalisation des jeunes;

Niveau 8 : Surveiller les jeunes ayant des antécédents criminels ou des problèmes de santé mentale qui semblent enclins à rallier des groupes extrémistes, et préparer des programmes d'activités spéciaux (sports, formation professionnelle, etc.) à leur intention;

Niveau 9 : Offrir des mesures incitatives aux membres désabusés pour qu'ils quittent leur groupe terroriste, puis publier leurs témoignages avec leur accord et les aider à démarrer une nouvelle carrière;

Niveau 10 : Offrir des récompenses aux membres du public qui fournissent des informations contribuant à prévenir une attaque terroriste ou conduisant à l'arrestation d'extrémistes violents et de terroristes;

Niveau 11 : Assurer la surveillance et le suivi de certains délits ordinaires (comme le vol d'explosifs) qui pourraient être commis pour préparer une attaque terroriste;

Niveau 12 : Établir des protocoles d'intervention rapide pour traiter les alertes crédibles transmises (dans les médias sociaux, entre autres) par l'auteur des faits ou le porte-parole d'une organisation terroriste;

Niveau 13 : Utiliser les médias et les réseaux sociaux pour alerter la population lorsque des informations crédibles font état d'une attaque terroriste imminente et lui demander d'être vigilante, d'essayer de repérer les suspects dont l'identité est connue et les objets suspects et de les signaler, le cas échéant, aux intervenants en utilisant la ligne téléphonique spéciale mise en place à cet effet.

4.1.2.1 Concevoir une stratégie relative aux cibles vulnérables

Dans les Principes directeurs relatifs aux combattants terroristes étrangers, connus sous le nom de Principes directeurs de Madrid[27], les États Membres sont invités, de concert avec les autorités locales, « à élaborer, mettre en œuvre et en pratique des stratégies et des plans d'action pour réduire les risques d'attaques terroristes contre les infrastructures critiques et les cibles vulnérables, qui associent et mobilisent les moyens des parties prenantes compétentes, tant publiques que privées. » [S/2018/1177, annexe, principe directeur 50 c)].

27 Les 27 et 28 juillet 2015, le Comité contre le terrorisme a tenu une réunion spéciale à Madrid afin de discuter du suivi de la résolution 2178 (2014) du Conseil de sécurité concernant la meilleure manière d'endiguer le flot de combattants terroristes étrangers. Les représentants des États Membres, d'organisations internationales et régionales, du milieu universitaire et de la société civile présents ont défini 35 principes directeurs (Principes directeurs de Madrid) (S/2015/939, annexe II). Le 13 décembre 2018, le Comité a tenu une autre réunion spéciale au cours de laquelle il a créé un additif aux principes directeurs existants, prévoyant 17 nouveaux principes (S/2018/1177, annexe).

Pour établir les stratégies nationales, il est recommandé de consulter les services gouvernementaux, les entités du secteur privé/exploitants de sites et les organisations de la société civile (voir section 4.2.2). Ces stratégies doivent répondre à un ensemble de questions essentielles comme :

- Qu'entend-on par « cible molle » et quels critères devraient être utilisés pour les repérer ?
- De quelle façon le contexte de menace à l'égard des cibles molles sera-t-il défini et évalué ?
- Quels sont les rôles et les responsabilités des différents ministères et niveaux de gouvernement (c'est-à-dire les autorités fédérales, infranationales, régionales et locales) pour ce qui est de faire face à la menace et de réagir à un incident ?
- Quelles autorités doivent participer à la gestion des risques et des crises, et quelles procédures doivent être mises en place à cette fin ?
- Quelles formes de partenariats public-privé pourrait-il être utile d'établir (notamment avec les exploitants de sites), comment les parties prenantes du secteur privé seront-elles identifiées, et quels canaux permettront un échange d'informations efficace entre les secteurs public et privé ? (voir encadré 3)
- De quelle façon les organisations de la société civile et le grand public seront-ils amenés à participer à l'effort de protection ?

Encadré 3.
Partenariats public-privé pour la protection des cibles molles – UNICRI

Les Principes directeurs de Madrid, en particulier les principes 50 et 51 (voir S/2018/1177, annexe), recommandent aux États Membres de définir leur approche à l'égard des partenariats public-privé visant à protéger les cibles vulnérables en se fondant sur les mesures suivantes :

- Créer des mécanismes ou renforcer les mécanismes existants qui permettent aux parties prenantes tant publiques que privées de mettre en commun leurs informations, leurs compétences (telles que des outils et des directives) et leurs expériences aux fins des activités d'enquête et d'intervention en cas d'attaques terroristes visant de telles cibles [50, g)];
- Établir des procédures permettant au gouvernement et aux secteurs industriel et privé de mettre en commun leurs évaluations des risques, afin de favoriser, mieux comprendre et renforcer la sécurité et la résilience des cibles vulnérables [51, c)];
- Établir des procédures en vue d'échanger des informations avec les partenaires des secteurs industriel et privé, par exemple par la délivrance d'habilitations de sécurité ou des campagnes de sensibilisation [51, d)];
- Faciliter les partenariats public-privé par l'élaboration de mécanismes de coopération, l'appui aux chefs d'entreprise et aux gestionnaires d'infrastructures, et la mise en commun, le cas échéant, de plans, de politiques et de procédures [51, e)].

La stratégie globale applicable aux cibles molles dans différents secteurs et domaines d'activité donnera donc les grandes lignes qui serviront à élaborer des sous-stratégies et des plans d'action ciblés. Cette stratégie devra en outre être compatible avec celles de nature analogue que pourraient adopter les gouvernements dans des domaines connexes, tels que la protection des infrastructures critiques, la lutte contre le terrorisme, la sécurité nationale et la gestion des crises. L'élaboration d'une stratégie nationale relative aux cibles molles peut même être l'occasion de revoir l'ensemble des stratégies et des plans d'action connexes en vue d'assurer l'harmonisation des opérations et la coordination entre les multiples parties prenantes, de simplifier les procédures et d'optimiser l'utilisation des ressources.

Étude de cas 1.
Stratégie de l'Australie pour protéger les lieux très fréquentés contre les actes terroristes

La stratégie de l'Australie pour protéger les lieux très fréquentés contre les actes terroristes repose sur l'établissement de partenariats solides basés sur la confiance entre tous les niveaux de gouvernement et les responsables de ces lieux (propriétaires et exploitants). Son objectif est d'optimiser la résilience des lieux très fréquentés face aux attaques terroristes tout en préservant l'utilisation et la jouissance de ces lieux.

Cette stratégie adoptée en 2017 repose sur quatre principes : 1) établir des partenariats plus solides; 2) favoriser un meilleur échange d'informations et une meilleure orientation; 3) mettre en œuvre des mesures de sécurité préventive efficaces; 4) accroître la résilience.

Source : Stratégie de l'Australie pour protéger les lieux très fréquentés contre les actes terroristes (2017).

Étude de cas 2.
Aperçu du plan de sécurité des cibles molles et des lieux très fréquentés (Département de la sécurité intérieure des États-Unis)

Dans cet aperçu du plan, on présente brièvement l'approche adoptée par le Département de la sécurité intérieure des États-Unis pour coordonner sa mission, qui consiste à renforcer la sécurité et la résilience des cibles molles et des lieux très fréquentés.

La gestion des risques et des crises est fondée sur les principes suivants :

- La mission est un effort partagé des parties prenantes (comprenant le grand public, les propriétaires et les exploitants de ces sites/lieux, les partenaires du secteur de la sécurité, les partenaires gouvernementaux aux niveaux étatique, local, tribal et territorial, et le gouvernement fédéral);
- Le rôle du Département est d'assurer la sécurité des lieux dont il est responsable et d'aider les autres parties prenantes à s'acquitter de leurs responsabilités liées à la sécurité des sites dont elles sont responsables. Pour ce faire, il a recours à quatre axes d'action : 1) opérations de sécurité directes dans des installations et des emplacements qui peuvent être considérés comme des cibles molles ou des lieux très fréquentés, comme les infrastructures de transport, les ports, les voies navigables, etc.; 2) sensibilisation, renseignement et échange d'informations;

(suite)

3) renforcement des capacités et des aptitudes des partenaires; 4) recherche et développement.

Le Département de la sécurité intérieure mène plusieurs initiatives qui ont notamment pour but :

- de mettre en valeur une culture de vigilance dans le cadre d'une importante campagne d'éducation et de sensibilisation;
- de s'engager à échanger des pratiques exemplaires et des enseignements avec des partenaires internationaux clés;
- de mieux faire connaître les ressources du Département en ce qui concerne les cibles molles et les lieux très fréquentés et de les rendre plus accessibles en élaborant des guides de ressources, des directives en matière d'auto-assistance, etc.;
- de concentrer et d'encourager les investissements dans la sécurité des cibles molles et des lieux très fréquentés, en tirant parti des subventions et de l'assistance technique offertes pour en améliorer la sécurité et favoriser les investissements dans ce domaine;
- d'axer les activités de recherche et développement sur la sécurité des cibles molles et des lieux très fréquentés.

Source : Département de la sécurité intérieure des États-Unis (2018).

Outil 4.
Handbook to Assist in the Establishment of Public-Private Partnerships to Protect Vulnerable Targets (Manuel visant à faciliter l'établissement de partenariats public-privé pour protéger les cibles vulnérables) – UNICRI (2010)
(https://unicri.it/topics/public_private_security_policies)

L'UNICRI a élaboré ce manuel en 2010 à la suite d'une série d'ateliers, de réunions d'experts, d'analyses pragmatiques et de tests. Il a été conçu à l'intention des responsables de la sécurité au sein des entités publiques et des entreprises privées et vise à leur offrir, de manière sensée et pragmatique, une méthodologie en dix étapes et des outils qui peuvent être utilisés pour établir des partenariats public-privé ou renforcer ceux existants afin de prévenir les menaces liées à la sécurité aux niveaux national et local et de répondre à ces menaces.

Il est un complément, et non un substitut, aux dispositions ou aux plans nationaux ou régionaux existants en ce qui a trait à la protection des « cibles molles » vulnérables.

Outil 5.
Mémorandum d'Antalya, section B – Édifier des partenariats public-privé – Forum mondial de lutte contre le terrorisme (2017)
(www.thegctf.org/Portals/1/Documents/Framework%20Documents/2017/GCTF%20Antalya%20Memorandum%20FR.pdf?ver=2020-10-07-144133-960)

La section B du Mémorandum est consacrée à l'établissement de partenariats public-privé pour assurer et améliorer la coopération dans le domaine de la sécurité ainsi qu'à la mobilisation des entreprises au moyen de messages clairs et cohérents sur la nature de la menace et le niveau adéquat de préparation. Les bonnes pratiques décrites à cet égard sont les suivantes :

Bonne pratique n° 6 : Faire intervenir toutes les parties prenantes à l'établissement d'un cadre national antiterroriste qui délimite clairement les responsabilités en matière de préparation : prévention, protection, atténuation, réponse et relèvement.

Bonne pratique n° 7 : Améliorer la coopération entre les agences gouvernementales et en leur sein, à tous les niveaux, ainsi qu'avec le secteur privé, et renforcer les échanges d'information et le partage d'expériences entre les États.

Bonne pratique n° 8 : Établir une relation de confiance entre les pouvoirs publics et les entités privées du secteur de la sécurité et encourager le secteur privé à jouer un rôle proactif dans les efforts de sécurité.

Bonne pratique n° 9 : Tout citoyen et tout employé du secteur privé peut contribuer à la sécurité en signalant les activités suspectes.

4.1.2.2 Déterminer ce qui constitue une cible molle

Dans sa résolution 75/291, l'Assemblée générale a exhorté les États Membres à « redoubler d'efforts pour améliorer la sécurité et la protection des cibles particulièrement vulnérables, y compris les sites religieux, les établissements d'enseignement, les sites touristiques, les centres urbains, les manifestations culturelles et sportives, les pôles de transport, les rassemblements, les cortèges et les convois, ainsi que pour renforcer leur résilience face aux attaques terroristes, en particulier dans le domaine de la protection des civils » (par. 71). Dans l'additif aux Principes directeurs de Madrid (S/2018/1177), le Conseil de sécurité a invité les États Membres à « recenser [...] les cibles vulnérables au niveau national, en procédant à une analyse continue des moyens dont disposent les terroristes, de leurs intentions et de leurs attaques passées » [principe directeur 50 b)]:

Bien que tout lieu puisse en théorie faire l'objet d'une attaque, les ressources limitées qui peuvent être consacrées à la sécurité imposent l'adoption d'une approche pragmatique reposant sur la hiérarchisation des cibles. Il est fondamental de recenser au préalable les sites qui courent le plus grand risque afin de prendre des décisions éclairées et fondées sur le renseignement pour déterminer quelles ressources sont nécessaires, ainsi que où et quand les déployer à des fins de prévention, de répression et de gestion de crises. Il est également essentiel de comprendre l'évolution du paysage terroriste, ainsi que l'intention et les capacités des auteurs de menaces sur le territoire des États Membres afin de repérer les nouvelles cibles molles ou celles devenues prioritaires.

Pour citer le Mémorandum d'Antalya du Forum mondial de lutte contre le terrorisme, les « cibles civiles ne sont pas spécifiques, elles sont en fait n'importe quel endroit où se rassemble ou se réunit un grand nombre de personnes. C'est la raison pour laquelle le concept de protection, loin d'être statique et axé sur un objet spécifique, doit être dynamique, réfléchi et organisé par zone géographique. » (Bonne pratique nº 4).

En outre, alors que la plupart des infrastructures critiques demeurent vulnérables en permanence puisque les exploitants sont censés assurer la continuité de services essentiels, les sites généralement définis comme des cibles molles ne deviennent souvent vulnérables que ponctuellement (notamment à l'occasion d'événements particuliers, tels qu'un concert ou l'ouverture d'un marché extérieur certains jours de la semaine)[28]. Par conséquent, les mesures de sécurité peuvent varier dans le temps et être adaptées à l'utilisation des lieux[29].

La densité de la foule constitue assurément un critère important pour déterminer si un endroit donné doit être qualifié de cible molle et faire l'objet de mesures de sécurité renforcées. Ce critère ne peut toutefois pas être le seul utilisé pour évaluer le niveau et les mesures de protection que requiert un site donné; d'autres indicateurs doivent être pris en compte, comme l'attrait particulier que présente un endroit ou un événement pour les terroristes en raison, par exemple, de sa valeur symbolique. Il faut aussi tenir compte du résultat de l'analyse de la menace nationale ou locale confirmant que certains sites pourraient être la cible d'une attaque.

Comme il est essentiel d'évaluer les conditions locales et les scénarios de menace pour pouvoir qualifier une zone de cible molle, les parties prenantes locales – y compris les exploitants du site et les autorités – constituent des acteurs clés dans le cadre des efforts de hiérarchisation, compte tenu de leur connaissance approfondie de la dynamique locale, du mouvement des foules, du calendrier des événements, etc., et de leur accès direct aux informations connexes.

4.1.2.3 Établir un cadre institutionnel et opérationnel pour la gestion des risques et des crises

Dans sa résolution 2396 (2017), le Conseil de sécurité souligne la nécessité pour les États Membres d'élaborer, de réviser ou de modifier les évaluations nationales des risques et des menaces pour tenir compte des cibles vulnérables en vue d'établir des plans d'urgence et des plans d'intervention d'urgence adéquats en cas d'attentats terroristes (14e alinéa du préambule).

Cette recommandation a été approfondie dans les Principes directeurs de Madrid, où les États Membres sont invités à élaborer des mesures visant à protéger les cibles vulnérables en procédant « à des évaluations régulières des risques afin de s'adapter à la nature changeante de la menace et de l'adversaire, y compris en utilisant les outils et les directives mis au point par les organisations internationales et régionales » [S/2018/1177, additif, principe directeur 50 b)].

Le principe directeur 51 recommande que, pour protéger les cibles vulnérables contre les attaques terroristes, les États Membres, agissant de concert avec les autorités locales, devraient également :

28 Comme mentionné à la section 1.2, les cibles molles et les infrastructures critiques sont protégées pour des motifs différents, qui supposent que les critères utilisés pour qualifier certaines infrastructures de critiques (à savoir l'ampleur des dommages qu'une attaque causerait à l'économie, à l'environnement, etc.) peuvent ne pas convenir pour déterminer les cibles molles.

29 Certains sites, par exemple, peuvent devenir soudainement vulnérables, notamment lorsque les autorités publiques sont informées de l'heure et du lieu d'une manifestation.

a) mettre à jour les plans d'intervention d'urgence, notamment les directives, les exercices et la formation à l'intention des services de répression, d'autres autorités compétentes et acteurs du secteur, afin de tenir compte des menaces réelles, d'affiner les stratégies et de faire en sorte que les parties prenantes s'adaptent à une menace en constante évolution;

b) instaurer des cadres et des mécanismes nationaux qui permettent d'accompagner le gouvernement et les acteurs du secteur dans la prise de décisions après évaluation des risques, l'échange d'informations et la création de partenariats public-privé, notamment pour qu'ils déterminent ensemble les priorités et élaborent conjointement les produits et outils utiles, tels que des directives générales sur la surveillance ou des suggestions de mesures de protection propres à différents types d'installations (par exemple les stades, les hôtels, les centres commerciaux ou les écoles);

c) établir des procédures permettant au gouvernement et aux secteurs industriel et privé de mettre en commun leurs évaluations des risques, afin de favoriser, mieux comprendre et renforcer la sécurité et la résilience des cibles vulnérables;

d) établir des procédures en vue d'échanger des informations avec les partenaires des secteurs industriel et privé, par exemple par la délivrance d'habilitations de sécurité ou des campagnes de sensibilisation.

Toute stratégie nationale concernant les cibles molles vulnérables doit établir que le cadre de gestion des risques et des crises est un exercice collaboratif qui repose sur les résultats des évaluations de menaces menées au niveau du gouvernement (national et local), du secteur (par exemple, les menaces propres à certains sites – lieux religieux, centres d'éducation, attraits touristiques, centres urbains, etc.) et des opérateurs de sites individuels. Comme les organisations de la société civile ont des rapports étroits avec les communautés locales et possèdent une expertise ciblée en ce qui concerne les questions de sécurité, il est essentiel de solliciter leur participation dès les premiers stades de la planification de la stratégie nationale.

Étude de cas 3.
Plan Vigipirate (France)

En France, le plan Vigipirate offre le cadre organisationnel et opérationnel lié à la gestion des risques et des crises qui sert à assurer la protection contre le terrorisme. Ce plan requiert la participation de l'État, des autorités locales, des entreprises et des citoyens. Les attaques terroristes perpétrées au pays en 2015 et 2016 contre plusieurs cibles vulnérables ont conduit à une révision du plan Vigipirate pour l'adapter à une menace particulièrement élevée. La version actuelle du plan repose sur trois piliers :

1. Le développement d'une culture de la sécurité individuelle et collective élargie à l'ensemble de la société civile;
2. La création de trois niveaux adaptés à la menace et matérialisés par des identifiants visibles dans l'espace public :
   a) Le *niveau de vigilance* correspond à la posture permanente de sécurité et à la mise en œuvre de 100 mesures différentes;

(suite)

b) Le *niveau sécurité renforcée – risque d'attentat* adapte la réponse de l'État à une menace terroriste élevée, voire très élevée. Plusieurs mesures particulières additionnelles peuvent alors être activées en complément des mesures permanentes de sécurité et selon les domaines concernés par la menace;

c) Le *niveau urgence attentat* peut être mis en place à la suite immédiate d'un attentat ou si un groupe terroriste identifié et non localisé entre en action. Ce niveau est mis en place pour une durée limitée : le temps de la gestion de crise. Il permet notamment d'assurer la mobilisation exceptionnelle de moyens, mais aussi de diffuser des informations susceptibles de protéger les citoyens dans une situation de crise;

3. La mise en œuvre de nouvelles mesures renforçant l'action gouvernementale contre le terrorisme.

Concrètement, les analyses de la menace réalisées par les services de renseignement compétents permettent au Secrétariat général de la défense et de la sécurité nationale (SGDSN)[30] d'établir une posture générale de sécurité Vigipirate. Cette posture spécifie également les mesures devant être mises en œuvre :

- à l'occasion de grands événements nationaux (compétitions sportives, sommets internationaux, etc.);
- à certaines dates clés de l'année (rentrée scolaire et fêtes de fin d'année);
- après un attentat, en France ou à l'étranger, pour adapter, en urgence, le dispositif national de protection.

30 Le SGDSN est un organe interministériel qui relève du Premier Ministre et qui aide le Chef du Gouvernement à concevoir et à mettre en œuvre des politiques de défense et de sécurité.

En tout, le plan Vigipirate comprend environ 300 mesures parmi lesquelles des mesures permanentes appliquées à 13 grands domaines d'activité (transports, santé, etc.) et des mesures complémentaires activées en fonction de la nature et du niveau de la menace terroriste évaluée. Une partie de ces mesures sont classifiées. Le plan est prolongé dans certains domaines par des plans d'intervention spécifiques qui mettent en œuvre des moyens spécialisés (plans NRBC, Piratair-Intrusair, Pirate-mer, Piranet, Metropirate, Interception prolifération).

Source : Comprendre le plan Vigipirate (2021) (www.gouvernement.fr/risques/comprendre-le-plan-vigipirate).

Étude de cas 4. **Rapport sur l'identification des risques au niveau national (Agence suédoise pour la protection civile)**

À la demande du Gouvernement, l'Agence suédoise pour la protection civile a exposé en 2011 les grandes lignes d'une évaluation nationale des risques dans un rapport fondé sur une sélection de risques cernés par les autorités gouvernementales et les conseils administratifs des comtés. Ces risques couvrent un large éventail d'incidents, dont le terrorisme et les cyberattaques.

Le rapport présente également certains cas typiques où la Suède pourrait avoir à faire une demande d'assistance internationale. Les annexes décrivent des scénarios antérieurs qui ont été évalués à l'aide de diverses méthodes.

Source : Rapport sur l'identification des risques au niveau national (2011).

4.1.2.4 Établir une politique de communication

Il est important que des stratégies de communication[31] soient mises en œuvre à toutes les étapes du processus de gestion des risques et des crises et que tous les organismes gouvernementaux s'accordent sur les faits et la démarche à suivre. En plus d'informer les diverses catégories de parties prenantes et de les tenir au fait de la situation en temps de crise et tout au long du cycle de sécurité, les plans de communication doivent viser à préserver la cohésion sociale et éviter de stigmatiser certaines communautés.

Toute stratégie de communication doit définir les mécanismes qui seront utilisés pour mobiliser l'ensemble de la population et les modalités qui s'appliqueront. Le Mémorandum d'Antalya du Forum mondial de lutte contre le terrorisme présente des bonnes pratiques que les gouvernements peuvent adopter avant, pendant et après une attaque contre une cible molle (voir Bonne pratique nº 13) :

Avant un attentat : Partager des évaluations réalistes des risques en vue de gérer les attentes de la population. Le but est d'optimiser l'utilité des alertes et d'éviter que les terroristes ne parviennent à répandre un sentiment d'insécurité. La difficulté pour les pouvoirs publics est de parvenir à informer la population et formuler des conseils utiles sans se faire involontairement l'écho du message des terroristes, submerger l'opinion publique d'informations incessantes ou éroder la vigilance[32];

Pendant un attentat : Définir comment réagir et les informations à diffuser. Dans le plan d'intervention, le volet communications compte autant que les détails opérationnels. Il faut fournir des instructions claires à la population au sujet des zones à éviter, des refuges disponibles et d'autres informations pratiques, sans toutefois amplifier le message des terroristes, comme on l'indiquait plus haut;

Après un attentat : Le retour à la normale doit se faire aussi vite que possible. Il faut être prêt à communiquer sur les médias sociaux et préparer les messages qui seront diffusés lors d'un attentat avant que celui-ci ne survienne. Il est également crucial de procéder à l'évaluation des plans de communication immédiatement après un attentat, afin de tirer des enseignements.

4.1.3 Forces de l'ordre

Les principaux rôles et responsabilités des forces de l'ordre en ce qui concerne la protection des cibles molles peuvent être regroupés en trois grands ensembles d'activités :

1. *Soutenir les exploitants de cibles vulnérables :* les forces de l'ordre sont appelées à offrir différents types de soutien qui peuvent les amener, entre autres, à préparer des évaluations de la menace/vulnérabilité et des plans d'urgence; à contribuer à l'organisation d'exercices et de formations à l'intention des employés des sites et du personnel de sécurité; et à aider à trouver des sources de financement en vue d'améliorer la sécurité. Si les exploitants de sites vulnérables font confiance aux forces de l'ordre, il est plus probable qu'ils collaborent de manière proactive avec ces

31 Le Centre des Nations Unies pour la lutte contre le terrorisme du Bureau de lutte contre le terrorisme dirige un projet sur la prévention de l'extrémisme violent par des communications stratégiques, qui pourrait se révéler intéressant et utile dans ce contexte. Voir www.un.org/counterterrorism/cct/strategic-communication.

32 Sur le plan préventif, le Mémorandum d'Antalya du Forum mondial de lutte contre le terrorisme décrit également des techniques de communication que les gouvernements peuvent employer pour aider et inciter la population à détecter les menaces. La Bonne pratique nº 9 suggère que « la signalétique d'avertissement, les affiches et les publicités dans les transports en commun ou dans les lieux publics peuvent contribuer à sensibiliser la population à la question. Quant aux campagnes d'information, elles peuvent aussi y contribuer si elles sont bien ciblées. La radio et la télévision peuvent également diffuser des messages d'intérêt public. Dans les pays qui ne sont pas dotés d'un plan de communication publique, l'organisation régulière de réunions présentielles avec les représentants d'organisations professionnelles ou avec les propriétaires et exploitants des sites pour lesquels il existe des inquiétudes constitue un bon point de départ. »

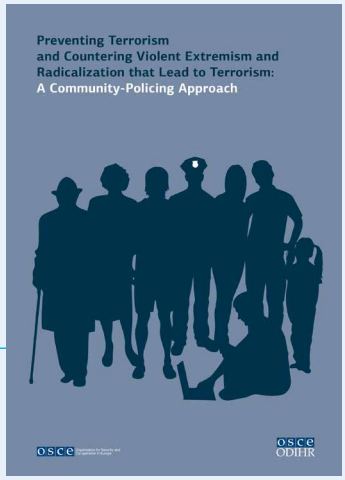
dernières sur les questions de sécurité, ce qui améliorera l'appréciation de la situation et la préparation des autorités;

2. *Enquêter sur les attaques terroristes contre des cibles vulnérables ou leur préparation :* les forces de l'ordre devraient étendre leurs enquêtes aux grands réseaux qui ont organisé ou aidé à préparer une attaque. Le succès de ces enquêtes repose sur la capacité des services de renseignement compétents à déterminer la probabilité d'une attaque et fournir des informations sur les déplacements des personnes surveillées. En outre, les agents de la justice pénale doivent connaître les processus de coopération internationale, comme l'entraide judiciaire, l'échange d'informations entre services de police, l'extradition ainsi que le traitement, la conservation et l'échange de preuves, qui seront utilisées dans le cadre de procédures pénales[33];

3. *Sensibilisation communautaire :* sur la base de l'expérience de plusieurs parties prenantes, le Mémorandum d'Antalya du Forum mondial de lutte contre le terrorisme souligne l'importance de faire appel à des chargés de liaison de la police pour interagir avec les populations locales, expliquer les lois et aider les personnes (en particulier les immigrants) à comprendre quels sont leurs droits et leurs devoirs; c'est là « une mesure essentiellement préventive qui vise à détecter et résoudre les problèmes avant qu'ils ne dégénèrent. » (Bonne pratique n° 9). La sensibilisation communautaire est un aspect important des activités de police de proximité. Elle s'inscrit dans une grande stratégie policière reposant sur la collaboration et les partenariats entre les forces de l'ordre et les communautés locales.

Outil 6.

Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach (Prévention du terrorisme et lutte contre l'extrémisme violent et la radicalisation qui y conduisent : une approche de police de proximité) – Organisation pour la sécurité et la coopération en Europe (OSCE) (2014)
(www.osce.org/files/f/documents/1/d/111438.pdf)



Ce guide se situe au carrefour de trois priorités thématiques importantes pour l'OSCE qui ont récemment été réaffirmées par les États participants : 1) la lutte contre l'extrémisme violent et la radicalisation qui conduisent au terrorisme, en suivant une approche multidimensionnelle; 2) la promotion et la protection des droits humains et des libertés fondamentales dans le contexte des mesures de lutte contre le terrorisme, qui sont des priorités stratégiques de l'OSCE en matière de lutte contre le terrorisme, comme indiqué dans le Cadre consolidé de l'OSCE pour la lutte contre le terrorisme (décembre 2012); et 3) les partenariats

33 Lorsque les attaques contre des cibles vulnérables revêtent une importante dimension transnationale, notamment lorsque les victimes sont des ressortissants de plusieurs pays différents, les acteurs de la justice pénale des pays touchés peuvent envisager d'appliquer des mécanismes tels que le transfert des procédures pénales afin de regrouper efficacement les procédures sur un même territoire.

(suite)

police-public/police de proximité, qui sont l'une des priorités thématiques définies dans le Cadre stratégique de l'OSCE pour les activités relatives à la police (juillet 2012).

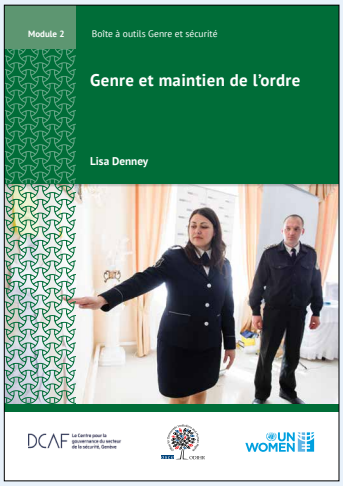
Le guide fournit des orientations générales concernant les facteurs importants qui peuvent influencer (positivement ou négativement) la capacité d'une approche de police de proximité à prévenir le terrorisme et lutter contre l'extrémisme violent et la radicalisation qui y conduisent. Il est donc destiné principalement aux décideurs et aux policiers hauts gradés, mais il peut également s'avérer utile pour les membres de la société civile qui s'intéressent à ces questions, en particulier pour les dirigeants communautaires. Il peut servir de référence commune qui rapprochera la police et les membres du public et les aidera à dialoguer sur le terrorisme et l'extrémisme violent et la radicalisation qui y conduisent. Il aborde les thèmes suivants :

- Concepts clés liés à la prévention du terrorisme et approches communautaires à la lutte contre le terrorisme;
- Mesure dans laquelle la police de proximité peut bénéficier des efforts de prévention du terrorisme et de lutte contre l'extrémisme violent et la radicalisation qui y conduisent;
- Recommandations visant l'intégration des normes relatives aux droits humains et à l'égalité des genres dans les activités de police de proximité;
- Conseils pratiques sur des questions liées à la mise en œuvre, telles que la coordination, l'attribution des tâches, la négociation, la communication, l'échange d'informations, la mobilisation de groupes spécifiques et les évaluations.

S'inspirant de publications précédentes de l'OSCE, le guide s'appuie sur une analyse de l'expérience accumulée par plusieurs États participants et partenaires pour la coopération de l'OSCE.

Outil 7.

Genre et maintien de l'ordre – Centre de Genève pour la gouvernance du secteur de la sécurité (DCAF), Bureau des institutions démocratiques et des droits de l'homme (BIDDH) de l'OSCE, ONU-Femmes (2019)
(https://dcaf.ch/sites/default/files/publications/documents/GSToolkit_Tool-2%20FR%20FINAL.pdf)



Le module Genre et maintien de l'ordre fait partie de la Boîte à outils Genre et sécurité, qui comporte neuf modules et une série de notes de synthèse. « Pour garantir l'égalité des genres dans et par le maintien de l'ordre, il ne suffit pas d'augmenter le nombre de femmes. Il faut

transformer les rapports de force qui perpétuent l'inégalité et la violence liée au genre. L'objectif est de protéger les droits humains de toute la population et de donner à toutes et à tous la possibilité de participer pleinement à la vie publique. S'il s'agit d'une obligation en vertu des législations nationales et internationales, intégrer une perspective de genre dans les services de police permet également d'assurer un maintien de l'ordre plus efficace, pour des sociétés plus sûres et un état de droit plus solide. » (voir Présentation, p. 1).

La boîte à outils présente un éventail d'options pour intégrer une perspective de genre et faire progresser l'égalité des genres dans et par le maintien de l'ordre, en s'appuyant sur l'expérience issue d'une variété de situations. Elle fournit des orientations sous forme d'exemples, d'aide-mémoire et de bonnes pratiques.

4.1.4 Premiers secours

Lorsque un attentat terroriste survient, il est essentiel que l'intervention des premiers secours soit rapide et efficace afin d'atténuer l'impact de la crise et de bien enclencher le processus de relèvement[34]. Pour cela, il est important que tous ceux qui interviennent lors d'une attaque contre une cible molle – pompiers, police, services d'urgence et de santé :

1. aient recours à des systèmes de communication interopérables[35];
2. prennent contact avec les exploitants de sites bien avant un incident afin de se familiariser avec les particularités des sites et ainsi être en mesure de fournir une aide plus rapidement et plus efficacement en cas d'urgence;
3. fassent participer les exploitants de sites à des exercices et à des simulations pour s'assurer qu'ils sont prêts si les procédures d'urgence (évacuation du site, par exemple) devaient être enclenchées;
4. envisagent de désigner un responsable/point de contact et veillent à ce que les exploitants de sites sachent quelle personne ou quel organisme contacter pour discuter des mesures de sécurité, notamment de préparation et de protection.

Encadré 4.
Une notion élargie de l'interopérabilité

L'interopérabilité s'entend généralement de la capacité technique des systèmes de communication à se connecter les uns aux autres et à interagir. Cependant, la notion d'interopérabilité est en pleine évolution; elle s'élargit pour couvrir l'interopérabilité des équipes, la synchronisation des procédures et l'harmonisation des pratiques d'échanges d'informations en s'appuyant sur les préceptes suivants :

34 Parallèlement, il est essentiel que les premiers secours planifient et réalisent leurs interventions en étant conscients qu'ils peuvent eux-mêmes devenir la cible de violences terroristes s'il y a une deuxième attaque alors qu'ils sont en train de porter secours aux victimes. Une analyse constante de la menace changeante que représentent les acteurs terroristes s'impose.

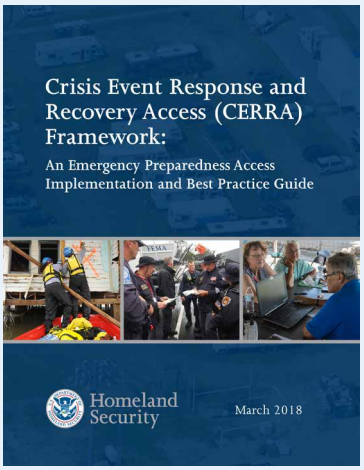
35 Dans les Principes directeurs de Madrid, les États Membres sont invités à « encourager une plus grande interopérabilité dans le domaine de la gestion de la sécurité et des crises » [principe directeur 50 e)].

(suite)

- Aller au-delà de la technologie : rendre les personnes et les procédures interopérables et créer une culture d'interopérabilité;
- Agir de façon délibérée : confier à un organisme ou à une unité, comme seul mandat, l'interopérabilité et l'intégration opérationnelle. Élaborer des solutions faciles à déployer;
- Faire preuve de diligence : s'assurer que les nouveaux systèmes informatiques, la formation et le personnel sont orientés vers l'interopérabilité. S'assurer que les fournisseurs sont en mesure de tenir leurs promesses;
- Se préparer : effectuer des exercices mettant exclusivement l'accent sur l'intégration des fonctions critiques entre les organismes;
- Être son pire critique : produire des rapports rétrospectifs pour tous les exercices et incidents, établir des plans d'amélioration qui reflètent la réalité sur le terrain et formuler des attentes raisonnables;
- Faire de l'interopérabilité une priorité en matière de sécurité publique : des secouristes bien protégés seront mieux à même de protéger à leur tour les populations auprès desquelles ils interviennent.

Source : Intervention de M. Donell Harvin, de l'Université de Georgetown, lors de la réunion du Groupe d'experts sur la protection des centres urbains et des sites touristiques, organisée par le Bureau de lutte contre le terrorisme les 15 et 16 juin 2021 (voir www.un.org/counterterrorism/events/international-expert-group-on-protection-urban-centres-touristic-venues).

Outil 8.
Crisis Event Response and Recovery Access (CERRA) Framework (Cadre sur l'accès aux ressources pour réagir aux crises et les surmonter) – Département de la sécurité intérieure des États-Unis (2018)
(www.cisa.gov/publication/crisis-event-response-and-recovery-access)



Ce cadre fournit une orientation aux autorités compétentes pour les aider à contrôler et à coordonner de manière sûre et efficace l'accès aux principales ressources disponibles dans une zone affectée pour réagir à une situation d'urgence et la surmonter. Il présente des mécanismes, des outils, des processus et des approches pour coordonner, approuver et faciliter l'accès aux ressources pendant les opérations de secours et de relèvement.

4.1.5 Services de renseignement

En raison de leur mandat de maintien de la sécurité nationale, les services de renseignement sont appelés à jouer un rôle essentiel dans la collecte et l'analyse d'informations sur les transactions, les conversations, les déplacements d'individus et les mouvements de marchandises qui peuvent être révélateurs de l'orchestration d'actes terroristes contre des cibles vulnérables. Ils jouent également un rôle important dans l'analyse de l'évolution de la menace terroriste, notamment en ce qui a trait aux intentions et aux capacités. Les services de renseignement devraient toujours s'acquitter de leur mandat en respectant l'état de droit, l'égalité des genres et les obligations internationales relatives aux droits humains[36]. Toutes les activités de surveillance doivent respecter les normes internationales de droit à la vie privée et être soumises à des mécanismes de contrôle efficaces et indépendants. Les rôles et responsabilités des services de renseignement sont les suivants :

- Continuellement évaluer la nature générale et le niveau global de la menace, notamment en surveillant les plateformes sociales et en traitant les informations provenant d'acteurs non étatiques pour relever des indices signalant des comportements potentiellement violents. Cette tâche est souvent ardue, notamment lorsque des individus se radicalisent en peu de temps et ne font pas officiellement partie d'une organisation terroriste;
- Infiltrer les groupes terroristes – et leurs plateformes sociales – en vue d'en apprendre davantage sur leur structure, leurs intentions, leurs ressources, leurs capacités, leurs plans pour s'attaquer à des sites vulnérables, etc.[37];
- Exploiter les renseignements de sources publiques. Les renseignements n'ont pas forcément besoin d'être sensibles ou classifiés pour être utiles; les groupes terroristes ont souvent recours à des publications accessibles au public pour identifier leurs cibles et fournir des directives opérationnelles concernant leurs méthodes d'attaque;
- Établir ou consolider une relation de collaboration avec les forces de l'ordre, en particulier au niveau local, de même qu'avec les personnes qui exercent les fonctions de police de proximité. Ces personnes sont proches des populations locales, entretiennent avec elles des contacts étroits et connaissent le contexte local;
- Assembler des éléments d'information provenant de sources différentes et variées, et anticiper ce qui se trame (des renseignements concernant le vol de matières explosibles peuvent avoir un rapport avec d'autres liés aux déplacements de certains individus en direction ou en provenance de certains endroits, par exemple). Même les renseignements peu révélateurs peuvent faire partie de l'équation. Bien qu'ils ne signalent pas en soi une intention ou un comportement criminel, ils peuvent, une fois juxtaposés à d'autres données, révéler des menaces;
- Envisager de déclasser ou supprimer les renseignements confidentiels relatifs aux menaces pour les communiquer à d'autres autorités publiques et aux exploitants de

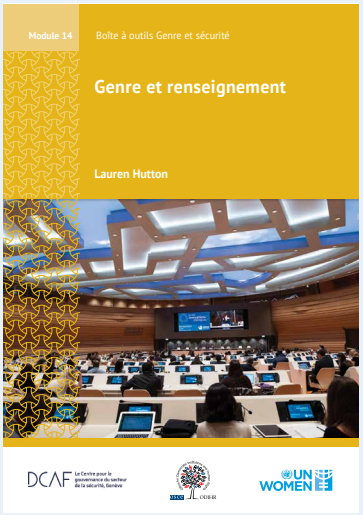
36 À la demande du Conseil des droits de l'homme, le Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans le cadre de la lutte antiterroriste, Martin Scheinin, a établi une « Compilation de bonnes pratiques en matière de cadres et de mesures juridiques et institutionnels, notamment de contrôle, visant à garantir le respect des droits de l'homme par les services de renseignement dans la lutte antiterroriste ». Les 35 bonnes pratiques qui y sont recensées sont le fruit d'une procédure de concertation avec les gouvernements, les experts et les praticiens. Voir A/HRC/14/46.

37 Les auteurs d'attentats terroristes annoncent souvent leurs intentions à l'avance sur les plateformes sociales. Parallèlement, plus les entreprises de médias sociaux traditionnelles deviennent efficaces pour contrôler le contenu publié sur leur plateforme, plus les discussions en rapport avec le terrorisme tendent à se dérouler sur des plateformes sociales marginalisées ou personnalisées, qui peuvent être plus difficiles à surveiller.

sites vulnérables afin d'assurer la gestion des risques[38];

- Intégrer les questions de genre dans la planification, la collecte, l'analyse et la diffusion des produits de renseignement afin de mieux détecter les signes d'instabilité négligés, traiter les données objectivement, acquérir une compréhension globale de la dynamique et des contextes sociaux, et anticiper et atténuer les conséquences négatives potentielles que la collecte et la transmission de renseignements peuvent avoir sur les droits civils, politiques et humains des personnes concernées.

Outil 9.
Genre et renseignement – DCAF, BIDDH de l'OSCE, ONU-Femmes (2019)
(https://dcaf.ch/sites/default/files/publications/documents/GSToolkit_Tool-14FR.pdf)



Le module Genre et renseignement fait partie de la Boîte à outils Genre et sécurité, qui comporte neuf modules et une série de notes de synthèse. Ce module en particulier est une ressource de bonnes pratiques à mettre en place lors de l'élaboration de politiques et de procédures et/ou lors d'une réforme du secteur du renseignement dans le but de faire progresser l'égalité des genres et d'intégrer une perspective de genre.

« Étant donné le caractère fermé et confidentiel du secteur du renseignement, les vastes initiatives du public et du secteur de la sécurité pour l'intégration d'une perspective de genre ont, pour la plupart, mis plus de temps à pénétrer le domaine du renseignement. Les travaux de réforme du secteur du renseignement ne comportent que très rarement des considérations liées au genre. Les efforts déployés pour contrer les déséquilibres de genre dans les services de renseignement sont relativement récents, et sont tributaires des perceptions sociétales plus vastes quant aux rôles sociaux de genre, des progrès en matière d'égalité des genres et du niveau de démocratisation. » (p. 2).

38 Dans sa résolution 2396 (2017), le Conseil de sécurité a exhorté les États Membres à envisager, le cas échéant, « de déclasser à des fins administratives les données de renseignement, y compris les données relatives aux voyages, sur la menace posée par les combattants terroristes étrangers et les terroristes, afin de communiquer ces informations au niveau national, de manière appropriée, aux services de contrôle de première ligne que sont l'immigration, les douanes et la sécurité des frontières, et de les transmettre comme il convient aux autres États et organisations internationales compétentes concernés, dans le respect des lois et politiques nationales et internationales, et de faire connaître leurs bonnes pratiques à cet égard » (par. 8).

4.2 Acteurs non étatiques

En ce qui concerne la protection des cibles vulnérables, dans sa résolution 75/291, l'Assemblée générale a demandé aux États Membres « de créer ou de renforcer les partenariats nationaux, régionaux et internationaux avec les parties prenantes, tant publiques que privées, selon qu'il conviendra, de mettre en commun leurs informations et leurs données d'expérience aux fins des activités de prévention, de protection, d'atténuation des effets, d'enquête, d'intervention et de rétablissement d'un fonctionnement normal en cas d'attaques terroristes » (par. 73). Les États Membres ont ainsi reconnu l'importance de mettre en place des partenariats multidimensionnels pour prévenir et contrer la menace contre les cibles vulnérables. La présente section traite de la manière dont les parties prenantes concernées peuvent soutenir les efforts de l'État à cet égard.

4.2.1 Exploitants de sites

Selon la nature du site considéré et les cadres réglementaires applicables, les exploitants de cibles vulnérables peuvent être des entités du secteur privé, des organismes publics ou des consortiums mixtes public-privé. Bien que les différentes catégories de parties prenantes soient assujetties à des cadres normatifs distincts, elles ont toutes un rôle essentiel à jouer pour que toutes les personnes présentes dans leurs installations (visiteurs, employés, artistes, etc.) bénéficient d'un environnement sûr et sécurisé.

Les principaux ensembles de responsabilités et recommandations connexes à l'intention des exploitants de sites sont les suivants :

- Réaliser des évaluations de la menace et de la vulnérabilité propres au site :
  - Examiner en quoi la nature particulière d'un site, son emplacement, sa taille, etc., et les vulnérabilités qui lui sont propres l'exposent à certains types de menaces;
  - Contacter les services de police locaux compétents pour obtenir des conseils afin de comprendre les menaces existantes, et aider à concevoir des plans de sécurité appropriés;
  - Tenir compte du fait que certaines mesures de sécurité conviennent à certains risques, mais pourraient être inutiles (voire contre-productives) face à d'autres. Les exploitants doivent relever le défi d'adapter le niveau de sécurité aux multiples menaces présentes[39];
  - Tester les hypothèses et instituer un programme centré sur les enseignements tirés de l'analyse d'attentats antérieurs[40]. Parallèlement, une analyse qui ne repose que sur des événements passés peut être contre-productive : « on s'attend à ce que les terroristes suivent le même *modus operandi*, et on sécurise les installations et on effectue les contrôles en conséquence. Il y a donc énormément de ressources consacrées à empêcher l'histoire de se répéter alors que les acteurs violents cherchent à s'en prendre aux États-Unis de manière inattendue ou asymétrique[41]. »

39 Par exemple, ajouter de la végétation dans les zones piétonnes peut limiter la vitesse à laquelle une attaque en voiture est perpétrée, mais aussi restreindre la capacité des caméras de vidéosurveillance à capter d'éventuels délits mineurs.

40 Mémorandum d'Antalya, Bonne pratique nº 11 : « Les enseignements tirés doivent ensuite être appliqués sur le terrain, puis il convient de déterminer ceux qui doivent continuer à faire partie de l'approche globale. Le recours à des "*Red teams*" (équipes qui adoptent le mode de pensée des terroristes et planifient des opérations en utilisant leurs tactiques en vue de chercher à exposer les vulnérabilités de leurs adversaires) peut aider les responsables de la sécurité à repérer les points faibles et à prévoir les améliorations à apporter en matière de réponse à un attentat et d'atténuation de son impact. Les *Red teams* peuvent également tester les réponses sécuritaires dans le cadre d'exercices contrôlés. »

41 Hesterman (2019), p. 21 et 22.

Encadré 5.
Promouvoir une planification de la sécurité des cibles vulnérables qui tient compte des questions de genre

Les politiques institutionnelles d'atténuation des risques doivent intégrer une analyse des questions de genre et aider les exploitants de sites à mieux tenir compte, dans leur planification, de la réalité des femmes en matière de sécurité. Mener systématiquement cette analyse peut grandement contribuer à la détermination de facteurs d'atténuation des risques, à l'efficacité des stratégies qui en découlent et à l'application de ces stratégies, tout en réduisant au minimum les répercussions sexospécifiques disproportionnées des mesures prises.

- Prendre des mesures appropriées d'atténuation des risques :
  - Appliquer le principe de la sécurité à niveaux multiples autour du site à protéger. Bien que le nombre, l'ampleur et la sophistication des mesures d'atténuation puissent varier, ce principe doit être appliqué à tous les sites, quelle qu'en soit la taille ou la complexité[42];
  - Examiner l'ensemble des mesures de sécurité envisageables et choisir la combinaison la plus appropriée selon les évaluations de sécurité, les normes contraignantes/recommandées et les ressources budgétaires. Les mesures de sécurité doivent être proportionnelles à la menace et mises en œuvre par des employés motivés et bien formés. Parmi les exemples figurent :
    > La sécurité au sens classique du terme (gardes, barrières, caméras de vidéosurveillance, etc.);
    > La « sécurité dès la conception » (c'est-à-dire la prise en compte de la sécurité dès les premières stades de conceptualisation des sites);
    > Les mesures destinées à contrer la menace que peuvent représenter les personnes qui cherchent à être recrutées (en tant qu'employés, bénévoles, travailleurs temporaires, etc.) ou à accéder autrement au site (en tant que prestataires de services extérieurs, par exemple) pour comprendre et étudier la dynamique et les processus internes afin de planifier un attentat (« menace interne »);
    > La cybersécurité : la dépendance croissante des systèmes à l'égard d'Internet (lecteurs de badges, caméras, etc.) signifie que les terroristes peuvent chercher à pirater ces systèmes pour obtenir l'accès au site sans être détectés;
    > Les outils de communication visant à dissuader les terroristes potentiels, dont l'utilisation d'outils trompeurs (comme de fausses caméras de sécurité à l'entrée du site ou des formulations sur le Web donnant à penser que le site est hautement sécurisé).
- Se préparer aux situations d'urgence :
  - S'assurer que des plans d'intervention d'urgence (pour l'évacuation des lieux, entre autres) sont en place et éprouvés;

42 Également appelée « défense en profondeur », la sécurité à niveaux multiples implique l'adoption de multiples mesures de sécurité, de sorte que si une mesure donnée échoue, la solidité des autres mesures peut tout de même contrer l'attaque ou en atténuer les conséquences.

– Aider le personnel de sécurité, les secouristes et les agents des forces de l'ordre compétents à se familiariser avec les particularités du site;
– Avec l'appui des agents des forces de l'ordre et des secouristes, organiser de manière proactive des exercices, des formations, des séances d'information, etc., au sujet des procédures d'urgence (notamment des évacuations) à l'intention des personnes présentes sur le site (personnel, visiteurs, etc.).

Encadré 6.
Sécurité des sites vulnérables : point de vue de l'exploitant

- La sécurité doit faciliter les activités, et non y nuire inutilement. Les mesures de sécurité doivent être proportionnelles au risque pour lequel elles sont conçues et tenir compte de l'incidence qu'elles peuvent avoir sur les visiteurs et de la façon dont ces derniers y réagiront.
- Un processus de contrôle approprié doit être élaboré afin de réduire les risques que des objets interdits soient introduits sur les lieux ou dans les aires de spectacle sans cependant nuire à l'expérience des visiteurs.
- Dans la mesure du possible, différents membres du personnel (coordonnateurs, personnel de sécurité, équipes responsables des relations avec la clientèle, etc.) doivent participer au maintien de la sécurité. Des chiens de recherche peuvent également être utilisés.
- Si possible, il faut déployer un système complet de vidéosurveillance et de contrôle des véhicules pour permettre aux personnes autorisées de circuler librement dans les zones adaptées à leur profil et leurs besoins.
- Il faut collaborer avec les forces de l'ordre, les services de sécurité, les autorités et les professionnels du secteur en vue d'évaluer et d'améliorer les mesures de sécurité de manière continue.
- Il faut veiller à ce que les membres du personnel du site soient suffisamment préparés et formés pour intervenir et porter secours lors d'un incident majeur. Les employés doivent être informés sur la menace du terrorisme et sur ce qu'ils peuvent faire pour prévenir ou empêcher une attaque, notamment en signalant les éléments suspects et en respectant les protocoles de sécurité.

Sources : Counter Terror Business (2020); Williams (2021).

Outil 10.
Sélection de ressources à l'intention des exploitants de cibles vulnérables – Département de la sécurité intérieure des États-Unis, Cybersecurity and Infrastructure Security Agency (CISA)

- Le site *Tools and resources to help businesses plan, prepare, and protect from an attack* (outils et ressources offerts aux entreprises pour les aider à planifier, à se préparer et à se protéger d'une attaque) renferme des conseils et des recommandations d'experts à l'intention du secteur privé et des partenaires communautaires concernant les mesures de protection qu'ils peuvent mettre en œuvre pour protéger leurs installations. Les entreprises sont encouragées à nouer des liens, à concevoir des plans, à former leurs employés, à s'exercer et à signaler tout élément suspect avant qu'un incident ou une attaque survienne. Cela permettra aux organisations et aux employés d'aborder leur rôle en matière de sécurité de manière proactive (www.cisa.gov/publication/connect-plan-train-report).
- La *Business Continuity Planning Suite* (trousse de planification de la continuité des opérations) aide les entreprises à créer, améliorer ou actualiser leur plan de continuité des opérations afin de réduire les répercussions potentielles de toute perturbation. Elle comprend une formation sur la planification de la continuité des opérations, des générateurs de plans de reprise après sinistre et de continuité des opérations, et un outil permettant de valider les plans de continuité (www.ready.gov/business-continuity-planning-suite).
- La vidéo *Check It!* sur le contrôle des sacs montre comment fouiller les sacs pour protéger les lieux et les clients (www.cisa.gov/video/check-it-bag-check-video).
- Le *Patron Screening Best Practices Guide* (guide des meilleures pratiques pour le contrôle des visiteurs) propose des moyens d'élaborer et d'appliquer des procédures de contrôle des visiteurs lors de grands événements sportifs, de concerts, de courses de chevaux, de cérémonies de remise de prix et d'autres rassemblements semblables (www.cisa.gov/publication/patron-screening-guide).
- La trousse de planification d'urgence en cas de fusillade décrit les concepts fondamentaux liés à l'élaboration d'un plan d'action d'urgence en cas d'une telle attaque, y compris les aspects importants à considérer. La trousse comprend notamment :
  - une vidéo qui explique les éléments importants de la conception d'un plan d'action d'urgence au moyen de témoignages de survivants, de secouristes et d'experts (www.cisa.gov/active-shooter-emergency-action-plan-video);
  - un guide qui fournit les renseignements nécessaires à l'élaboration d'un plan d'action d'urgence;
  - un modèle pour créer son propre plan d'action d'urgence (www.cisa.gov/publication/active-shooter-emergency-action-plan-guide).
- L'*Active Shooter Recovery Guide* (guide pour un relèvement efficace après une fusillade) montre comment mettre en œuvre des politiques et procédures qui aideront les entreprises à se remettre d'une fusillade tout en offrant la meilleure structure de soutien possible à leurs employés, leurs fournisseurs, leurs visiteurs, leurs clients, leurs familles et leurs communautés (www.cisa.gov/publication/active-shooter-recovery-guide).

- L'*Action Guide – Mass Gatherings: Security Awareness for Soft Targets and Crowded Places* (guide d'intervention pour les rassemblements de masse : sensibilisation à la sécurité des cibles vulnérables et des lieux très fréquentés) décrit comment les entreprises peuvent se préparer à d'éventuelles attaques et en atténuer les effets. Il présente aussi des mesures de protection essentielles à envisager (www.cisa.gov/sites/default/files/publications/Mass%20Gatherings%20-%20Security%20Awareness%20for%20ST-CP.PDF).
- Le site Web *What to Do – Bomb Threat* (mesures à prendre en cas d'alerte à la bombe) fournit des conseils et des ressources, notamment des procédures détaillées sur la manière de gérer les alertes à la bombe ainsi que les colis et les comportements suspects, et contient des informations pour aider à se préparer et à intervenir dans ce type de situation (www.cisa.gov/what-to-do-bomb-threat).
- Le guide *Best Practices for Mail Screening and Handling Processes* (meilleures pratiques liées au contrôle et au traitement du courrier) de l'Interagency Security Committee fournit aux gestionnaires, aux superviseurs et au personnel de sécurité des centres postaux un cadre pour comprendre et atténuer les risques organisationnels du courrier et des colis qui sont expédiés chaque jour (www.cisa.gov/sites/default/files/publications/isc-mail-handling-screening-nonfouo-sept-2012-508.pdf).
- La vidéo *Understanding the Insider Threat* (comprendre les menaces internes) fait appel à des experts en sécurité et en comportement pour discuter des différentes manières dont les menaces internes prennent forme, ce qui inclut le terrorisme, la violence au travail et les atteintes à la cybersécurité (www.cisa.gov/insider-threat-trailer-and-video).

4.2.2 Organisations de la société civile

Compte tenu de leurs divers domaines d'activité (recherche, politique, mobilisation de la population) et de spécialisation/expertise ainsi que de leur présence à différents niveaux (local, national, international), les organisations de la société civile ont des points de vue fort variés qui leur permettent de contribuer à la sécurisation des sites vulnérables. Elles apportent une valeur ajoutée à plusieurs égards, dont les suivants :

- Les organisations de terrain actives près de cibles vulnérables, ou qui s'occupent de projets bénéfiques pour certains quartiers ou certaines communautés, peuvent fournir des informations essentielles concernant les menaces locales. Elles peuvent également contribuer aux plans de sécurité des exploitants de sites ou des organismes gouvernementaux, que ce soit au niveau local ou national;
- Les organisations de la société civile assurent la prévention en amont des attaques terroristes par leur participation et leur soutien à des projets qui visent la déradicalisation et la réduction de l'attrait que présente l'extrémisme violent (voir étude de cas 5);
- Les organisations de la société civile peuvent assurer à divers titres la liaison entre les communautés locales auxquelles elles viennent en aide et les autorités publiques. Elles peuvent notamment porter les préoccupations des populations locales à l'attention des décideurs et contribuer à la diffusion et à la compréhension des directives de sécurité;
- Pendant ou après les crises, les organisations de la société civile peuvent apporter

un soutien essentiel aux victimes[43] et contribuer aux efforts de reprise économique et sociale (voir étude de cas 6);

- Les organisations de la société civile sont essentielles pour prévenir et apaiser les tensions intra et intercommunautaires en créant des espaces sûrs où discuter des problèmes et des préoccupations, en canalisant l'expression des dissensions et griefs et en facilitant l'échange d'expériences et de points de vue entre les membres du public;
- Les organisations de la société civile jouent également un rôle essentiel en faisant pression pour que les interventions juridiques, politiques et opérationnelles soient conformes aux normes de droits humains et d'égalité des genres[44].

Étude de cas 5.
Fonds mondial pour l'engagement de la communauté et la résilience

Créé en 2014, le Fonds mondial pour l'engagement de la communauté et la résilience est un mécanisme de financement international soutenu par 19 États, des organisations internationales, des fondations, des entreprises et des particuliers. Son objectif est de renforcer la résilience des communautés en subventionnant et en soutenant des initiatives locales visant à lutter contre les principales cause de l'extrémisme violent. Les subventions sont versées à des personnes morales constituées dans le territoire, aux bénéficiaires principaux responsables de la coordination d'un consortium d'organisations communautaires ou à des sous-bénéficiaires qui réalisent des activités de prévention de l'extrémisme violent. Le volet de financement accéléré et complémentaire offre aussi du financement d'urgence pour gérer les situations émergentes.

Le financement est accordé selon divers principes directeurs, dont les suivants :

- *Prise en main par le pays :* les activités qui sont menées par les communautés locales soutiennent les objectifs stratégiques des gouvernements nationaux;
- *Pertinence du contexte :* les décisions de financement sont fondées sur des évaluations approfondies des facteurs locaux qui mènent à l'extrémisme violent;
- *Responsabilisation et apprentissage :* les méthodes et outils utilisés sont continuellement évalués pour être améliorés.

Source : Fonds mondial pour l'engagement de la communauté et la résilience (www.gcerf.org).

43 Les victimes de violations des droits humains ont droit aux garanties suivantes : a) accès effectif à la justice, dans des conditions d'égalité; b) réparation adéquate, effective et rapide du préjudice subi (restitution, indemnisation, réadaptation, satisfaction et garanties de non-répétition); c) accès aux informations utiles concernant les violations et les mécanismes de réparation en vertu du droit international (voir résolution 60/147 de l'Assemblée générale, annexe, Principes fondamentaux et directives concernant le droit à un recours et à réparation des victimes de violations flagrantes du droit international des droits humains et de violations graves du droit international humanitaire, par. 11).

44 Lors de la réunion du Groupe d'experts international sur les cibles vulnérables et les systèmes de drone aérien tenue les 6 et 7 octobre 2021, plusieurs organisations de la société civile ont insisté sur ce point. Voir www.un.org/counterterrorism/events/international-expert-group-meeting-vulnerable-targets-and-unmanned-aircraft-systems. Les observations de la Rapporteuse spéciale sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste se sont révélées particulièrement importantes dans ce contexte. Voir www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/remarks_of_the_un_sr_ct_hr_at_the_egm_vulnerable_targets_and_uas.pdf.

Étude de cas 6.
Gérer les traumatismes causés par des actes terroristes (Centre pour les traumatismes et la résilience (NATAL), Israël)

Fondé en 1998, le centre NATAL est une organisation apolitique israélienne qui fournit des services aux victimes directes et indirectes de traumatismes, dont les victimes d'actes terroristes. Il œuvre sans distinction de religion, d'origine ethnique, de couleur de peau, d'âge, de genre ou de statut socioéconomique.

Ses objectifs sont les suivants :

- Servir de centre de traitement multidisciplinaire, grâce à une unité clinique composée de 150 thérapeutes dans tout le pays qui s'occupent des différents aspects des soins psychologiques et du soutien émotionnel;
- Venir en aide à la communauté en renforçant sa capacité de résilience face aux menaces actuelles, et contribuer aux interventions menées et aux efforts de relèvement déployés lors des situations d'urgence nationale. Le programme d'action communautaire comprend une unité mobile qui offre un traitement à domicile aux personnes et aux familles qui, en raison de la gravité de leur traumatisme, se sentent incapables de quitter leur foyer;
- Offrir aux anciens combattants, par l'entremise de son centre de témoignage, la possibilité de documenter sur pellicule les traumatismes qu'ils ont vécus, sous la supervision d'un professionnel de la santé mentale;

(suite)

- Mieux faire connaître les traumatismes causés par des actes terroristes et mettre fin aux préjugés à l'égard des personnes qui ont besoin d'aide psychologique. En organisant plusieurs campagnes et événements chaque année, l'unité des relations publiques et des services d'aide aux victimes de traumatismes touche des milliers de personnes de tous âges.

Source : NATAL (www.natal.org.il/en).

4.2.3 Secteur privé (à l'exception des exploitants de sites)

« Afin de protéger au mieux les cibles vulnérables, il faut nouer des partenariats public-privé ou renforcer ceux qui existent déjà, à tous les niveaux de décision, y compris au niveau de l'État, des collectivités locales et des autorités provinciales. Les États Membres devraient encourager et soutenir les partenariats avec les entreprises qui peuvent contribuer à tous les aspects de la préparation, à savoir la protection, l'atténuation des effets, les interventions et le rétablissement d'un fonctionnement normal après une attaque terroriste, ainsi qu'aux enquêtes menées sur de tels actes. » (S/2018/1177, par. 53).

Un large éventail d'entités du secteur privé jouent un rôle déterminant dans l'atténuation du risque d'attaques contre des cibles vulnérables, qu'elles agissent de leur propre chef, dans le cadre de partenariats public-privé volontaires ou sur le fondement de cadres réglementaires contraignants. Quoique non exhaustifs, les exemples qui suivent illustrent la diversité des entreprises qui peuvent contribuer à la protection des sites vulnérables :

- Les exploitants de cibles vulnérables ont souvent recours à des entreprises de sécurité privées pour diverses tâches de protection des personnes et des biens (contrôle d'accès aux sites, gardes, services de patrouille, sécurité informatique, conseils concernant l'amélioration de la sécurité, etc.). Qu'elles exercent un rôle opérationnel ou consultatif, ces entreprises peuvent renforcer la sécurité en se concertant avec les forces de l'ordre, en

particulier dans les pays où la menace terroriste est importante et où les capacités des organismes de sécurité publics sont déjà exploitées au maximum. Toutefois, elles doivent être adéquatement formées pour apporter une véritable valeur ajoutée à l'effort global de protection des cibles vulnérables. En outre, leurs rôles et responsabilités doivent être clairement définis dans les cadres juridiques applicables et codes de conduite complémentaires (voir encadré 7). La réglementation efficace de ces entreprises permet de garantir des normes professionnelles de base pour leurs employés et de définir clairement leur relation avec la police, les premiers secours et les autres autorités publiques responsables de la protection des cibles vulnérables.

Encadré 7.
Code de conduite international des entreprises de sécurité privées

Certaines organisations ont élaboré des lignes directrices et des programmes de certification pour garantir la qualité et le professionnalisme des services offerts par les entreprises de sécurité privées. Le Code de conduite international des entreprises de sécurité privées a notamment été adopté en 2010 à la suite d'une initiative multipartite lancée par le Gouvernement suisse[45]. Il prévoit un mécanisme d'adhésion volontaire (et ne vise donc pas à remplacer les cadres juridiques nationaux) qui soutient les efforts visant à garantir que les entreprises de sécurité privées ne négligent pas les droits humains. Les entreprises signataires « affirment qu'elles ont la responsabilité de respecter les droits humains de toutes les personnes affectées par leurs activités commerciales, à savoir leur personnel, leurs clients, leurs fournisseurs, leurs actionnaires et les populations des zones dans lesquelles elles fournissent leurs services, et d'assumer leurs responsabilités humanitaires à l'égard de ces personnes. Elles reconnaissent qu'il est important qu'elles respectent les cultures et les personnes avec lesquelles leurs activités les mettent en contact. » (par. 4).

À ce jour, plusieurs centaines d'entreprises ont adhéré au Code. De plus, l'ONU a rendu l'adoption obligatoire pour offrir des services de sécurité privés aux organismes des Nations Unies.

En 2013, un accord a été conclu concernant la Charte du mécanisme de gouvernance et de contrôle du Code. Ce mécanisme « prévoit des fonctions pour la certification des entreprises de sécurité privées, le monitoring et le traitement des plaintes, afin d'assurer la mise en œuvre effective [du Code][46] ».

45 https://icoca.ch/wp-content/uploads/2020/07/icoc_french3.pdf.

46 www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-47889.html.

- Les entreprises qui sont situées à proximité de sites vulnérables ou qui leur fournissent des biens ou des services peuvent contribuer à la détection et au signalement d'activités suspectes. Elles peuvent également participer aux efforts de gestion des crises, notamment en abritant les personnes évacuées sous la supervision des forces de l'ordre et des services de secours compétents;
- Les chauffeurs et autres employés des entreprises de transport adéquatement formés sur la reconnaissance et le signalement d'activités suspectes sont souvent bien placés pour contribuer à la prévention, étant témoins de ce qui se passe dans la rue et ayant un contact direct avec leurs passagers;
- Au vu des récentes attaques contre des sites vulnérables menées à l'aide de véhicules loués, les agences de location de véhicules peuvent faire une part du travail en amont en vérifiant plus en profondeur les antécédents de leurs clients[47]. Des mesures préventives semblables peuvent également être prises par d'autres entreprises qui gèrent des matières et des biens à double usage, ainsi que par les vendeurs et les détaillants de systèmes de drone aérien qui peuvent se retrouver entre les mains d'acteurs hostiles;
- En coordination avec les pouvoirs publics, les entreprises du secteur technologique peuvent tirer parti des fonctions de communication, de géolocalisation et d'algorithme de leurs plateformes en ligne pour fournir des services aux communautés touchées pendant ou après une crise (voir encadré 7);
- Les restaurants et services annexes peuvent prendre des mesures pour atténuer le risque de se voir exploités par des terroristes cherchant à contaminer la nourriture distribuée dans les écoles, les sites religieux, les centres de loisirs et de réadaptation, etc.

47 Dans ses Conclusions sur la protection des espaces publics (juin 2021), le Conseil de l'Union européenne a encouragé les États membres « à continuer d'étudier et d'analyser les orientations et outils en matière de sécurité destinés aux opérateurs de location de véhicules afin de prévenir et d'atténuer le risque d'attaques menées à l'aide de véhicules dans des espaces publics » (annexe, par. 29).

Encadré 8.
Les outils Facebook qui facilitent l'intervention lors d'une crise

Les Services de crise de Facebook sont une plateforme qui regroupe en un seul et même endroit les outils de sécurité suivants :

- **Contrôle d'absence de danger :** permet aux utilisateurs touchés par une catastrophe de faire savoir à leurs amis et à leur famille qu'ils sont en sécurité. Cette fonction peut être activée automatiquement lorsqu'il y a un afflux de publications d'utilisateurs et que l'incident est confirmé par une source gouvernementale ou une source d'information tierce[48];
- **Forum d'aide :** permet aux utilisateurs d'entrer en contact avec d'autres personnes présentes à proximité de la zone touchée en vue d'offrir ou de trouver de l'aide (pour de la nourriture, des fournitures, un refuge, etc.);
- **Collecte de fonds :** fournit un outil permettant de soutenir financièrement les personnes touchées par la crise;
- **Centre d'information :** fournit des liens vers des articles, des photographies et des vidéos afin d'aider les utilisateurs à en savoir plus sur la crise en cours au moyen de diverses sources.

Source : www.facebook.com/crisisresponse.

4.2.4 Utilisateurs de sites vulnérables

Les touristes, les fidèles réunis dans des lieux de culte, les visiteurs de lieux emblématiques dans les centres urbains, entre autres, ne sont pas seulement des cibles potentielles d'attaques terroristes, ils sont également des acteurs clés de la sécurité des sites qu'ils fréquentent et peuvent contribuer à limiter les répercussions d'une éventuelle crise. En particulier :

- On peut apprendre aux utilisateurs de sites vulnérables – et au public en général – à repérer toute dynamique inhabituelle, comme la « surveillance préopérationnelle », à la signaler et, potentiellement, à se mobiliser. On ne saurait surestimer l'importance d'une telle formation, surtout à une époque où les progrès technologiques permettent aux terroristes potentiels de surveiller leur cible de manière de plus en plus inaperçue[49];
- Lors d'une crise, les personnes présentes sur les lieux peuvent être en mesure d'apporter les premiers secours avant l'arrivée des forces de l'ordre et du personnel médical. Il peut donc s'avérer essentiel pour atténuer les répercussions d'une crise que les personnes qui fréquentent régulièrement des sites vulnérables acquièrent des connaissances générales de secourisme et de soins d'urgence.

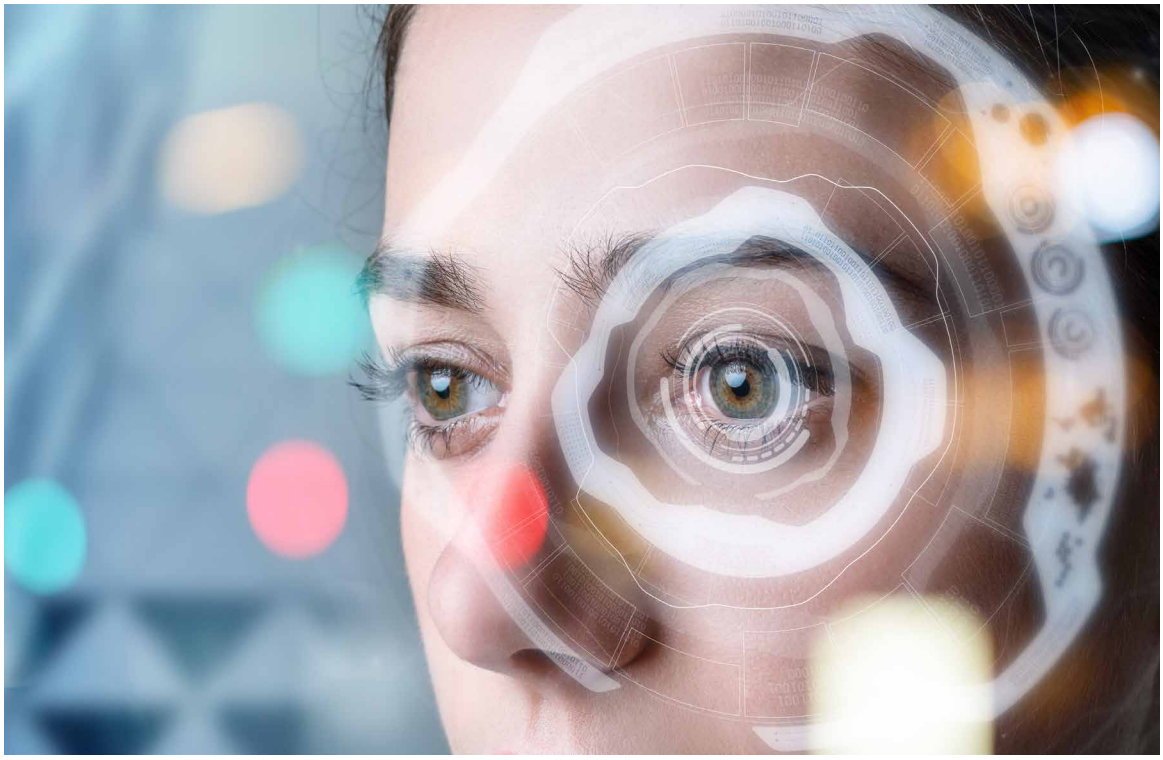
48 La fonction de contrôle d'absence de danger de Facebook a été activée lors de l'attentat-suicide à la bombe survenu à l'aéroport international de Kaboul le 26 août 2021 (voir www.cnet.com/news/facebooks-safety-check-activated-after-deadly-attack-outside-kabul-airport).

49 Par exemple, les systèmes de drone aérien, de plus en plus souvent équipés de moteurs silencieux, permettent de prendre des photos détaillées à une grande distance. Par ailleurs, des caméras discrètement intégrées dans des lunettes sont en vente libre.

Encadré 9.
Les répercussions sur les droits humains des politiques et des pratiques visant à repérer les signes de radicalisation

La Rapporteuse spéciale sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste a exprimé de sérieuses préoccupations aux approches qui « consiste[nt] à mettre à contribution la société tout entière aux fins de la détection des "signes de radicalisation", y compris les enseignants, les travailleurs sociaux, le personnel médical et les autres professionnels de la santé, le personnel pénitentiaire, les chefs de communautés, les membres de groupes religieux, et les voisins et les proches des personnes concernées [...] Elles détruisent la fragile confiance dont jouissent ces professionnels, dont le principal devoir est de protéger et d'autonomiser ceux dont ils s'occupent, alors qu'identifier les extrémistes restera quasiment impossible tant qu'on ne disposera pas de données scientifiques permettant de comprendre comment une personne bascule dans l'extrémisme violent. Les approches "globales" entraînent des signalements excessifs fondés en grande partie sur des motifs discriminatoires interdits, ce qui a des répercussions sur les droits à la liberté de religion, à la liberté d'expression et à la vie privée. »

Source : A/HCR/43/46, par. 32.



Outil 11.
Sélection de ressources à l'intention des utilisateurs de cibles vulnérables – Département de la sécurité intérieure des États-Unis

- La campagne nationale « **If You See Something, Say Something** » (si vous voyez quelque chose, dites quelque chose) vise à sensibiliser le public aux signes de terrorisme et de crimes connexes ainsi qu'à l'importance de signaler toute activité suspecte aux forces de l'ordre locales et de l'État (www.dhs.gov/see-something-say-something/about-campaign);
- **Action Guide: Active Shooter Attacks: Security Awareness for Soft Targets and Crowded Places** (guide d'intervention en cas de fusillade : sensibilisation à la sécurité des cibles vulnérables et des lieux très fréquentés) décrit les signes avant-coureurs d'une fusillade, ainsi que les mesures à prendre en cas d'incident. Il comprend aussi des conseils utiles pour concevoir des mesures de protection visant à prévenir de futures attaques (www.fema.gov/sites/default/files/2020-03/fema_faith-communities_active-shooter.pdf);
- **Le site Web Active Shooter Preparedness** (se préparer à une fusillade) permet d'accéder à divers produits, outils et ressources du Département de la sécurité intérieure pour se préparer et savoir comment réagir en cas de fusillade (www.cisa.gov/active-shooter-preparedness);
- **Action Guide: Chemical Attacks: Security Awareness for Soft Targets and Crowded Places** (guide d'intervention lié aux attaques chimiques : sensibilisation à la sécurité des cibles vulnérables et des lieux très fréquentés) décrit des scénarios possibles et les symptômes d'exposition à des produits chimiques. Le guide explique également comment atténuer les effets de futures attaques et comment réagir en cas d'incident (www.cisa.gov/sites/default/files/publications/Chemical%20Attacks%20-%20Security%20Awareness%20for%20ST-CP.PDF);
- **Action Guide: Vehicle Ramming: Security Awareness for Soft Targets and Crowded Places** (guide d'intervention lié aux attaques au véhicule-bélier : sensibilisation à la sécurité des cibles vulnérables et des lieux très fréquentés) décrit les signes avant-coureurs d'une attaque au véhicule-bélier. Le guide propose également des stratégies d'atténuation et des mesures de protection à envisager (www.cisa.gov/sites/default/files/publications/Vehicle%20Ramming%20-%20Security%20Awareness%20for%20ST-CP.PDF);
- **Action Guide: Mass Gatherings: Take Charge of Your Personal Safety** (guide d'intervention lié aux rassemblements de masse : prendre sa sécurité personnelle en main) décrit les signes avant-coureurs d'une attaque lors d'un rassemblement de masse et des mesures à prendre en réponse à un tel incident (www.cisa.gov/sites/default/files/publications/Mass%20Gatherings%20-%20Take%20Charge%20of%20Your%20Personal%20Safety.pdf).

Références

Agence suédoise pour la protection civile (2011). *A first step towards a national risk assessment: National risk identification* (www.msb.se/siteassets/dokument/publikationer/english-publications/a-first-step-towards-a-national-risk-assessment---final.pdf).

Australia-New Zealand Counter-Terrorism Committee (ANZCTC) (2017). *Australia's Strategy for Protecting Crowded Places from Terrorism* (www.nationalsecurity.gov.au/crowded-places-subsite/Files/australias-strategy-protecting-crowded-places-terrorism.pdf).

Centre de Genève pour la gouvernance du secteur de la sécurité (DCAF), Bureau des institutions démocratiques et des droits de l'homme (BIDDH) de l'OSCE et ONU-Femmes (2019). *Genre et maintien de l'ordre,* module 2, Boîte à outils Genre et sécurité.

_____ (2019). *Genre et renseignement,* module 14, Boîte à outils Genre et sécurité.

Counter Terror Business (CTB) (2020). « The O2 and event security », entretien (février) (https://counterterrorbusiness.com/features/ctb-interview-o2-and-event-security).

États-Unis d'Amérique, Département de la sécurité intérieure (2018). *Soft Targets and Crowded Places Security Plan Overview* (www.cisa.gov/sites/default/files/publications/DHS-Soft-Target-Crowded-Place-Security-Plan-Overview-052018-508_0.pdf).

États-Unis d'Amérique, Government Accountability Office (GAO) (2012). *Nuclear Nonproliferation: Additional Actions Needed to Improve Security of Radiological Sources at U.S. Medical Facilities* (www.gao.gov/assets/gao-12-925.pdf).

Forum mondial de lutte contre le terrorisme (2017). *Mémorandum d'Antalya sur les bonnes pratiques relatives à la protection des cibles civiles dans le contexte de la lutte antiterrorisme* (www.thegctf.org/Portals/1/Documents/Framework%20Documents/2017/GCTF%20Antalya%20Memorandum%20FR.pdf?ver=2020-10-07-144133-960).

Hesterman, Jennifer (2019). *Soft Target Hardening: Protecting People from Attack*, Routledge.

Organisation pour la sécurité et la coopération en Europe (OSCE) (2014). *Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach.*

Williams, Paul (2021). Intervention du chef de la sécurité d'AEG Europe lors de la réunion du Groupe d'experts des Nations Unies sur la protection des centres urbains et des sites touristiques, organisée par le Bureau de lutte contre le terrorisme les 15 et 16 juin 2021 (voir www.un.org/counterterrorism/events/international-expert-group-on-protection-urban-centres-touristic-venues).

Pour en savoir plus, voir :

www.un.org/counterterrorism/vulnerable-targets

21-18451-1

NATIONS UNIES
BUREAU DE LUTTE CONTRE LE TERRORISME